C/M/S/
The alliance of major
European law firms

Technology Annual Review

A month by month review of selected technology legal news from 2007

2008

Contents

Foreword

Welcome to CMS Cameron McKenna's Technology Annual Review. The Review contains short, easy to read articles on topics of interest over the year. Topics in this year's Review include: selling spam lists, illegal spyware, software copyright, VoIP, the i-Gasm, CD-WOW, the Fresh Prince, E-Commerce defences, data retention, digital downloads, domain name decisions, patent ambushes, the smiley :-), Bluetooth spam, and much, much more.

To provide industry focused advice to our clients we find it is important to keep up-to-speed with industry news as well as the legal news. This helps us to understand our clients' needs when working with them on complex transactions or when drafting agreements. Similarly, when we work with clients in relation to technology and media related disputes, our industry knowledge is invaluable when we are evaluating and formulating claims or when negotiating commercially viable settlements on behalf of clients.

If you would like to discuss any of the articles in this year's Review or any technology, media or telecoms law issue you or your business is facing, or you would like to talk to us about the services we can provide both in the UK and across Europe, please do not hesitate to contact us.

John Armstrong
john.armstrong@cms-cmck.com
+44 (0)20 7367 2701

Susan Barty
susan.barty@cms-cmck.com
+44 (0)20 7367 2430

Phillip Carnell
phillip.carnell@cms-cmck.com
+44 (0)20 7367 2430

Isabel Davies
isabel.davies@cms-cmck.com
+44 (0)20 7367 2156

Yuban Moodley
yuban.moodley@cms-cmck.com
+44 (0)20 7367 3453

Ian Stevens
ian.stevens@cms-cmck.com
+44 (0)20 7367 2597

Point v Focus: what was the point?

January

February

March

April

May

June

July

August

September

October

November

December

The Court of Appeal decision in *Point Solutions Limited v Focus Business Solutions Limited* was handed down in January. Both parties were suppliers of computer software and services in the financial services sector. The parties had entered into an outsourcing agreement under which Point was provided with some of Focus' software for review purposes. Prior to returning Focus' software, Point commenced work on a competing software product which it subsequently launched. Focus later sought confirmation from Point that they had not copied their software and proposed going to an independent expert to determine whether any copyright infringement had taken place. After prolonged correspondence, and attempts to appoint an independent expert to resolve the dispute, something unusual happened…

Point, the party accused of copyright infringement, took the decision to issue proceedings against Focus, asking the court for a declaration that Point's software did not infringe the copyright in Focus' software. At the first court hearing, the High Court refused to grant Point a declaration as Point had failed to prove a negative, namely that it had not copied Focus' software in creating its competing software. The High Court's refusal to grant a declaration was largely attributable to a lack of evidence. In reaching her conclusion, the trial judge pointed to the fact that Point had failed to call as witnesses the developers largely responsible for the development of the software and also questioned the reliability of the evidence given by the Point witnesses that were available. The judgment included the Judge's comment that: *"I am being asked to make a declaration that software, which I have not seen, does not infringe any copyright in another software product which I have not seen and in respect of which copyright has not been demonstrated."*

Point appealed to the Court of Appeal. The leading appeal Judge, Chadwick LJ, agreed largely with the trial Judge's findings and dismissed the appeal. He criticised the parties' failure to obtain an expert's report but also speculated that Point may have failed to appreciate the lacuna in its evidence – namely, the absence of evidence from those who had developed the software.

The futility of this claim was highlighted by the appeal Judge in his closing speech when he expressed regret as to the unsatisfactory outcome of this case. However, in his opinion, the outcome would have been equally unsatisfactory had a declaration been granted. The lack of an expert's report combined with the absence of evidence from key witnesses meant that the appeal Judge's conclusion was somewhat inevitable.

The judgment raises some interesting questions. Unlike trade mark, design and patent law, there is no prohibition on making unjustified threats of copyright infringement proceedings. What should a software developer do, therefore, when faced with untrue, but potentially public and damaging, claims of copyright infringement? One route would be to consider taking action for defamation or malicious falsehood, which can be effective if the allegations are clearly untrue or designed to damage. Another route is to take action akin to that taken by Point in this case. However, as with any copyright claim, it is important to bear in mind that expert evidence will probably be required before the court can make any final decision on infringement.

A good month for… 7 Seconds of Love

An unsigned London band reached an out-of-court settlement following a "David vs. Goliath" dispute with Coca-Cola. The dispute concerned an Argentinean diet coke advert that bore a striking resemblance to 7 Seconds of Love's song "Ninja" and their animated video for the song. Unfortunately for Coca-Cola, the band's video had been included in a weekly email (B3TA) which is sent to subscribers around the world. An Argentinean fan of the newsletter alerted the band to the copycat video.

A bad month for… Pecker

David Pecker, a publishing executive, failed to gain control of davidpecker.com as he could not prove he had trade mark or service mark rights in his name (i.e. he wasn't famous enough). According to WIPO, he could only demonstrate "broad assertions" that: he was known by the name nationally and internationally, he had a high profile in the publishing industry and he was regularly cited in the media. The website currently displays pornographic adverts and is held by a man in California. WIPO said only famous people who trade on their name have a chance of gaining control of a domain name containing their name.

Old McDonald sent some spam

Microsoft has succeeded in stopping a British man, Paul McDonald, from selling lists of email addresses through his company, Bizads, to spam distributors. To try and protect its customers, Microsoft brought proceedings against McDonald, claiming that he had failed to comply with the Privacy and Electronic Communications Regulations 2003 (PECR).

Broadly speaking, the PECR are designed to prevent the sending of unsolicited marketing messages unless the recipient has given the sender consent or has indicated that he does not, for the time being, object to receiving such communications. Microsoft brought an action against McDonald under the PECR for selling lists of email addresses that were then used as spam lists and claimed that McDonald's actions had caused it to suffer loss and damage to its goodwill as the owner of Hotmail.

The court said that complaints received from those people on the lists indicated that they had not consented to receiving the emails in question. It found that, as Microsoft had suffered a loss as a result of the breach of the PECR, it had a cause of action under the PECR. Further, the court said that even though McDonald did not send the unsolicited emails himself, it was able to characterise his actions as "instigating" spam for the purpose of the PECR. Consequently, the court granted an injunction preventing McDonald from instigating the transmission of spam to Hotmail accounts and ordered McDonald to pay compensation to Microsoft.

No E-Commerce defences for search engines

The Government declined to support a change to the UK's E-Commerce Regulations which would grant greater protection to search engines and other intermediaries. It said that such changes should be left to a European Commission review later in the year.

The liability of intermediaries hosting or caching information or acting as 'mere conduits' is limited under the E-commerce Directive (2000). However, although the protection granted to ISPs is relatively clear, the protection granted to search engines is much less so. Member States were given the choice of whether or not to grant protection to search engines and, consequently, protection has been granted in some Member States and not others and with inconsistent results.

In the UK, hosts are protected against copyright infringement actions to an extent but there is no explicit protection for search engines, providers of links or content aggregation services. The Government published a consultation paper in 2005 seeking views as to whether changes should be made.

Unsurprisingly, providers of the search and content aggregation argued for a specific extension of the e-commerce defences. The responses received from search engines indicated that they feared being made responsible for failing to filter, assess or censor content passed on to their users. Such responsibility, it was argued, would hinder the automated operation of their service. In contrast, content owners fighting against unauthorised use of their work, argued against an extension on the grounds that it would assist those distributing protected works without permission.

Ultimately, the Government decided against extending the limitations as there was insufficient evidence to warrant such an extension. In other words, no successful action had been taken against a search engine or content aggregation service in the UK and there was therefore no need to worry about it yet!

Patent asserted against Blackberry invalid on the ground of obviousness

January

February

March

April

May

June

July

August

September

October

November

December

The UK subsidiary of the manufacturer of the BlackBerry, RIM, sought revocation of a patent (owned by a patent holding company, Inpro) for a computing system that enables small computer devices to use the Internet. The system uses a proxy server to carry out much of the "heavy" computing in order to provide the portable computer with manageable content. Inpro, who appear to have been threatening patent infringement action against RIM and the network providers supplying the BlackBerry device, counterclaimed for patent infringement.

Section 1 of the Patents Act 1977 states that, amongst other things, a patent may only be granted for an invention which '*involves an inventive step*'. Further explanation is provided in Section 3: '*an invention shall be taken to involve an inventive step if it is not obvious to a person skilled in the art, having regard to any matter which forms part of the state of the art...*'. A patent that fails to involve this inventive step can be held invalid for '*obviousness*'.

The trial judge in the High Court found the patent to be obvious in consideration of the prior art, and also stated that an earlier decision to order the case to be determined by the streamlined procedure was, in retrospect, inappropriate. Inpro appealed and, in dismissing the appeal, the Court of Appeal upheld the High Court's decision.

The prior art cited proposed using a proxy server between an Internet web-server and a small field computer to reduce the amount of data that was downloaded to, and processed by, the limited resources of the smaller computer. The only differences between the prior art and the patent claims were that the field computer should tell the proxy computer the size of its screen capacity and that files should be combined in the proxy server so as to send fewer files to the smaller computer. The Court of Appeal noted that Inpro was far from establishing that these two differences involved an inventive step and was also of the view that the BlackBerry involved a vast amount of detailed implementation and design as well as the ideas that were the subject of the claim.

In addition, and interestingly to anyone involved in patent litigation, the Court of Appeal provided guidance on the use of the streamlined procedure. This was introduced in 2003, and was primarily intended for use in smaller patent cases. It requires factual and expert evidence to be in writing, limits or dispenses with disclosure and only allows cross-examination where necessary. Use of the Streamlined Procedure enables cases to come to trial in a shorter period of time and cuts down on the length of time that such trials take. The Court of Appeal commented that:

> *"The decision to use that procedure must depend on all the circumstances of the case, which in particular includes its commercial importance, degree of complexity, the commercial and financial position of the parties…parties should always consider (and discuss) whether it would be sensible to use it whatever the size of the case."*

The case represents an important victory for RIM as, had the patent been found valid, it would have threatened the continued use of the BlackBerry technology. It also provides important guidance on the use of the streamlined procedure which, while providing welcome speed and efficiency, may be unsuitable for complex cases of high commercial importance.

A good month for… Apple and, err, Apple

The long running trade mark dispute between Apple Corps (the record company formed by The Beatles) and Apple Inc (the US hardware and software company) finally came to an end this month. The dispute was over Apple Inc's use of its "Apple" logo in connection with its iTunes music download service which Apple Corps claimed infringed the terms of a 1991 co-existence agreement between the parties. The parties have come to a new agreement whereby Apple Inc. will own all of the trade marks related to "Apple" and will license certain trade marks back to Apple Corps. The other terms of the settlement are confidential.

A bad month for… online news publishers

The Press Complaints Commission (PCC) announced that material published on UK newspaper and magazine websites would now be included in its remit. This reflects the fact that online articles, blogs and podcasts often contain additional and more damaging material to that contained in the hard copy publication. The PCC did not introduce new provisions specially designed for online content. However, its existing Code of Practice dealing with accuracy, privacy and its rules on journalistic best practice now apply to online content.

The Spy Who Loved Me (and who really needs to let go!)

February saw Anthony Walters sentenced to four months' imprisonment for conspiring to install surveillance software ('spyware') on his wife's computer. He had wrongly suspected that his wife had concealed her true assets from him during divorce proceedings.

Walters met a representative of a detective agency (a serving police officer who had told his employers that he was unfit to work through sickness!) who suggested he install spyware on his wife's computer. Walters and his son arranged for the spyware to be installed on the computer, which was located at Walter's company premises.

Walters gave a prepared statement at Court where he admitted instructing the detective agency, through his son, but claimed that the computer in question was company property and that there was nothing illegal about monitoring its usage. He did, however, admit that staff had not been informed of any such monitoring and that no other staff had been subjected to this kind of surveillance.

The Court of Appeal decided not to reduce Walters' sentence despite various mitigating factors, including a letter from his wife where she stated she had forgiven him and was devastated to learn that he had been sentenced to imprisonment.

The Court of Appeal judgment concluded: *'The privacy of [information kept on computers] must be protected and it is vulnerable to the kind of unauthorised interference and intrusion that occurred in this case…a sentence of imprisonment for offences such as this was not wrong in principle'.*

And the "stating the obvious" award for 2007 goes to…

The High Court ruled that forwarding a business letter to a third party could constitute copyright infringement. When combined with the ease in which emails may be forwarded, this decision serves as a warning against forwarding emails without considering whether the original author has consented.

The case related to a dispute over the quality of roofing slates. During the period of the dispute, a letter produced by the executive vice president of a Danish company was passed on to a roofing contractor who then widely circulated the letter. The High Court held that the letter qualified for copyright protection and that the circulation of it amounted to copyright infringement and the misuse of confidential information.

Only those business communications that involve original skill or labour will be copyright protected. Originality is only required in the expression or execution of the thought; it does not require the thought itself to be original or inventive. In this case, the Judge observed, *"its production did involve a substantial degree of independent skill and labour…The effort expended…was clearly significantly more than trivial."*

Although this case concerned a letter, emails will enjoy the same rights with respect to copyright protection. This is likely to have an impact on most businesses especially since "forwarding" of emails has become so common. The ruling serves as a reminder to companies about their use of email and that the content and copyright ownership of any emails received should be considered before the "forward" button is pressed.

Nova v Mazooma

January

February

March

April

May

June

July

August

September

October

November

December

In March, the Court of Appeal handed down its judgment in *Nova Productions v Mazooma Games & Ors.* The appeal was brought against a first instance decision of the High Court which had decided that copyright in an arcade game, based on the game of pool, was not infringed by two competing arcade games, also based on the game of pool. Although the two allegedly infringing games were "inspired by" the first game, and incorporated some (but not many) similar elements, both the High Court and the Court of Appeal held that there was no copyright infringement.

The judgment was of significant interest and potential concern to software developers and the owners of copyright in computer programs. In its judgment, the Court of Appeal confirmed that:

- it is not an infringement of copyright to make a computer program which emulates another program (including its look and feel) but which does not copy the other program's code or graphics
- ideas which underlie computer programs are not protected by copyright
- no additional copyright protection, over and above protection as individual graphic works, is given to a series of images displayed in a computer program.

The judgment was handed down by three Court of Appeal judges, with the main judgment being given by Jacob LJ. The appeal was brought against a first instance decision of the High Court which had decided that copyright in an arcade game, based on the game of pool, was not infringed by two competing arcade games.

The Court of Appeal also tacitly approved the High Court decision in *Navitaire v easyJet* (2004), which reached the same conclusions in relation to software copyright. At the time it was made, the Navitaire judgment was considered to signal a death knell for any arguments that copyright could subsist in ideas underlying computer software or in the overall look and feel of software.

To add salt to Nova's wounds, when Nova requested that certain questions be referred to the European Court of Justice, the Judge replied that it was *"wholly unrealistic to suppose that the European Court of Justice would hold that copyright protection was to be given to ideas at such a high level of abstraction as those in this case".*

To protect the ideas underlying software, software developers could attempt to obtain patent protection for software. However, in Europe at least, patent protection is very difficult to obtain where the software does not form part of an invention which has a clear technical effect. Software developers and software copyright owners could also look to their licence agreements and insert contractual provisions to prevent the licensee from copying the software, even without copying the source code. However, such methods would offer no protection against third parties that are not licensees. However, without such measures, as a result of this judgment (and the previous judgment in *Navitaire*) it will be difficult for software copyright owners to take action against developers of software which has the same functionality, but which does not copy the underlying code or the graphics displayed on screen.

A good month for… Microsoft

Microsoft announced this month that it has reclaimed more than 1,100 infringing domain names set up by cybersquatters to target web users. The world's largest software provider went to war with US cybersquatters last August, filing multiple law suits to curb the number of cybersquatters using Microsoft brand names and phrases and common brand name misspellings in domain names. In addition to UDRP actions, in the US cyber-squatting is punishable by fine of up to $100,000 under the 1999 Anticybersquatting Consumer Protection Act. Companies therefore have a larger axe to wield in the US than in other jurisdictions.

A bad month for… Google

Google bought YouTube in October 2006 for $1.65 billion but six months later Viacom, which owns Dreamworks, Paramount Pictures and MTV, and a number of other cable channels, demanded that YouTube and parent company Google cough up $1 billion in damages. They contended that nearly 160,000 unauthorised clips of Viacom's entertainment programme were available on YouTube and that these clips had been viewed more than 1.5 billion times. They also asked the court for an injunction to halt the alleged copyright infringement immediately. Google downplayed the legal challenge but has reportedly set aside a very large sum of money to fund such claims.

Scottish spam

This month Gordon Dick (Edinburgh) won £750 plus costs from an English "marketing company" called Transcom Internet Services Ltd. This was the first action of its kind in Scotland and only the second in the UK so far, the first being last January where a Mr Roberts won £270 (plus £30 for costs).

Dick was sent the spam email in February 2006. After receiving the email he contacted Transcom seeking a promise to delete his personal data and also an explanation for their actions. Transcom wrote back confirming its responsibility for the email but denying that its actions were illegal and, playing a dangerous game, challenged Dick to sue. Dick filed a small claim in May 2006 taking action against Transcom for violations of the UK's Privacy and Electronic Communications Regulations 2003, which gives individuals (i.e. not businesses) the rights to avoid receiving spam over any private media from a spammer based in the UK.

Dick won a record amount of costs, £617, along with £750 damages, which reflects the dim light in which the court viewed Transcom's failure to settle the case at an earlier date. The main message from the decision though is that the courts will not accept this sort of breach of privacy.

Dick was able to take action because the spam was sent to his home email address and also that Transcom were based in the UK. Had either of those facts been different, he would not have had an action under the Regulations, which are impotent in respect of foreign (and therefore the majority of) spammers.

At risk of squatters

The World Intellectual Property Organisation (WIPO) released statistics this month which showed that there was a 25% increase in the number of cybersquatting disputes filed with WIPO during the previous year. This is evidence of more and more brand owners taking action against cybersquatters.

It appears that the recent changes allowing registrants to register names free-of-charge for a five-day "taster" period and the establishment of new Top Level Domains has created greater opportunities for the mass registration of domain names without specific consideration of third-party intellectual rights.

The concerned categories include, luxury items, famous persons, entertainment, hospitality, sports, gambling and pharmaceuticals and also charitable organisations and educational institutions, all of which can cause customer confusion.

In 2006, WIPO received 1,823 complaints alleging cyber squatting. A large number of the disputes related to newly merged or collaborating corporations which suggests that cybersquatters tend to follow the news and company announcements (note: for the sake of a £10 domain name registration fee, it is **always** worth registering a domain before announcing new brand names or company mergers!).

The report also revealed the interesting statistic that, since commencement in 1999, when applying the Uniform Domain Name Dispute Resolution Policy (UDRP), WIPO experts have resolved 84% of disputes in favour of the complaining party. Brand owners are therefore usually successful in obtaining domain names from cybersquatters. However, this may, of course, simply reflect the fact that UDRP complaints are only usually commenced where brand owners have good arguments in favour of a transfer.

Ofcom announces new regulatory code for VoIP

January

February

March

April

May

June

July

August

September

October

November

December

Voice over Internet Protocol (VoIP) services are having an increasing impact on the UK communications sector. Providers are offering increasing and significant benefits to consumers in the form of lower prices, more choice and new services.

In 2004 Ofcom published a consultation paper, "New Voice Services: A consultation and interim guidance". This paper set out Ofcom's proposals with regard to a future regulatory framework for VoIP services with the aim of maintaining consumer's interests. In the years leading up to the 2004 consultation, VoIP was a relatively infant market and did not have the capabilities and wide range of services and competitors that it does today.

In 2006 Ofcom published a second consultation paper, "Regulation of VoIP Services: Statement and further consultation", which took into account both the 2004 responses and developments in VoIP since 2004. The 2006 paper set out three objectives:

- Creating an innovative market in technology through regulation that avoids special treatment of one technology or another.
- Keeping consumers well informed.
- Maximising the availability of emergency services access.

To address these objectives, Ofcom proposed, first, to require providers of Public Electronic Communication Services to comply with a code of practice on the provision of customer information. Second, Ofcom proposed to modify the definition of a "Publicly Available Telephone Service" in Ofcom's General Conditions. This meant that only services available to the public for originating and receiving national and international calls with access to emergency services through a normal telephone number have the right to number portability.

A number of respondents to Ofcom's 2006 consultation expressed strong views about whether the proposed changes would be sufficient to ensure an adequately high level of access to emergency services for VoIP users. Despite this, the Code did not require VoIP providers to provide access to emergency services. However, VoIP providers were required to inform consumers whether or not the VoIP service offered has the capability to call emergency services; and also provide point of signature acknowledgement that access to emergency services is not possible in the case of a power cut.

Ofcom modified the definition of "Publicly Available Telephone Service", so that, unless a VoIP provider offers access to emergency services, it will not be able to offer customers the same number that they previously used with another service provider. Ofcom stated that it planned to issue a further consultation on emergency services access later in 2007. Indeed, later in the year it became a requirement on all VoIP providers charging a fee to provide access to the emergency services - see December's 'Good Month For' article.

Ofcom is also investigating other issues such as naked DSL, net neutrality and the regulation of nomadic services. With both the current and future increases in regulation, VoIP providers should ensure that they are well aware of what the regulations mean to them and how they will adapt to ensure compliance while continuing to grow and develop in the innovative VoIP market.

A good month for… sounding like you know what you are talking about when it comes to RFID

This month saw the Wireless Telegraphy (Radio Frequency) Identification Equipment (Exemption) (Amendment) Regulations come into force. The Amendment Regulations removed several technical restrictions relating to the shape of signal beams, the duration of signals and the operation of the "Listen Before Talk" protocol. The Amendment Regulations have been implemented as part of the drive towards European Harmonisation Standards (EN 302 208) and a more liberal approach to wireless telegraphy. One of the consequences is that it will be easier for some people to obtain licences under the Wireless Telegraphy Act 2006 for certain RFID equipment.

A bad month for… stealing your Internets

Police in Worcestershire arrested two people in unrelated incidents for illegally using another person's wireless Internet connection. The Communications Act 2003 makes an offence of dishonestly obtaining electronic communications services with the intent to avoid payment of a charge applicable to the provision of that service. Why should we be concerned that others are using our Wi-Fi? Well, if the person using your connection downloads unlawful material when doing so, you might have to suffer long cold night in police cell and have your own computer forensically scanned for evidence (and that is not even the worse case scenario!).

playboyracing.co.uk

A Nominet UK Dispute Resolution Service Appeal Panel decided that Playboy had rights in respect of the name and mark PLAYBOY, which was used in the domain name www.playboyracing.co.uk. The domain name was held to be an abusive registration and the panel directed the domain name should be transferred to Playboy Enterprises.

The respondent ran the website www.playboyracing.co.uk. Playboy claimed that the respondent was unjustly benefiting from the reputation in the PLAYBOY name and taking advantage of its rights.

Under paragraph 2(a) of the Policy, Playboy had to prove on the balance of probabilities that (i) it has rights in respect of a name or mark which was identical or similar to the domain name; and (ii) the domain name in the respondent's hands was an abusive registration.

Looking at the composite name, PLAYBOY RACING, the panel considered the word PLAYBOY to be the dominant and distinctive component of the domain name, as RACING was descriptive in nature. This satisfied paragraph 2(a)(i) of the Policy. When considering the abusive registration point, it was decided that the PLAYBOY brand would be blurred, diluted and devalued by the use of the domain name by the respondent – paragraph 2(a)(ii) of the Policy was therefore also fulfilled.

The decision serves as a warning to companies using names with considerable reputation and goodwill in which they have no rights – even as unconnected adjectives – in a domain name. It also boosts the armoury of those wishing to protect their brands from dilution and devaluation by non-related domain names.

High Court hears first FOIA case

The High Court made its first judgment in relation to the Freedom of Information Act 2000 (FOIA) in May 2007. The court considered both the issue of jurisdiction and the scope of "journalism". As a result, the rights of public service broadcasters to keep information from being released have been increased.

The BBC successfully appealed to the High Court against the Information Tribunal's decision in the action of Steven Sugar. He had requested information relating to Middle East news coverage.

The FOIA requires public authorities to disclose information they hold at the request of members of the public. The BBC is deemed to be such a "public authority" in respect of "information held for purposes other than those of journalism, art or literature."

The High Court held that, first, the decision as to whether information was of a journalistic nature, and therefore outside the scope of the FOIA, was to be taken by the Information Commissioner on a case-by-case basis. Secondly, because the Information Commissioner had decided that the information in this case did not fall within the scope of the FOIA, Sugar's appeal was not within the jurisdiction of the Information Tribunal, but that of judicial review proceedings.

One of the effects of the ruling is to remove a method of appeal for the public with respect to requests under the FOIA. However, it is good news for public service broadcasters as the decision reduces the likelihood of journalistic information in their hands being disclosed to the public.

Ministry of Justice consults on additional damages in copyright

January

February

March

April

May

June

July

August

September

October

November

December

The Ministry of Justice has published a consultation paper dealing with the law on damages, and has recommended that punitive damages should continue not to be awarded in civil claims against copyright infringers.

The Copyright Designs and Patents Act 1988 permits the award of "additional damages", as the justice of the case requires, in an action for copyright infringement. The term is unusual in English civil law, which refers elsewhere to restitutionary and aggravated damages. Restitutionary damages aim to compensate the victim for their actual loss, and aggravated damages aim to compensate a victim for injury to their feelings or mental distress caused or made worse by the wrongdoer's actions. The courts have not defined "additional damages" and have usually treated the phrase to mean restitutionary or aggravated damages.

The Ministry proposes replacing the term "additional damages" in the 1988 Act with the term "aggravated and restitutionary damages". Unlike the criminal law, civil law aims to compensate the victim rather than to punish the wrongdoer, and the Ministry, in excluding the possibility of punitive damages from the wording of the 1988 Act, aims to make clear the boundaries between the two.

The proposed change is welcome and is consistent with existing case law. The courts have previously awarded restitutionary or aggravated damages to claimants in civil actions where the defendant had calculated that the profit from its activities would exceed the amount of damages payable to the claimant. The Ministry's proposal would help to ensure that this policy applies equally in cases of copyright infringement. Damages would then be awarded on the same basis for the infringement of all intellectual property rights.

For IP rights holders, the proposal will allow for any damages awarded to include both a recovery of profits from the infringing party as well as aggravated damages. The existing position is that a Claimant must elect to receive either an account of profits or damages. The proposed changes should increase confidence in the ability of the current system of damages to have a dissuasive effect on potential infringers and will help to clarify the availability and extent of the damages available to both claimants and defendants.

Corporate IP rights holders will also welcome the Ministry's view that aggravated and restitutionary damages should also be made available to corporate as well as individual claimants. Previous case law has indicated that a company has no feelings to injure and is incapable of suffering distress, and therefore should not be entitled to aggravated and restitutionary damages. This has made it difficult for companies to claim additional damages for flagrant IP infringement, and the proposed change would increase the deterrent value of an IP infringement claim against a party responsible.

A good month for… proving that (some) lawyers have a sense of humour

The lawyers acting for Second Life, the Internet-based virtual world, have revealed themselves as having a sense of humour. Linden Labs contacted the website www.getafirstlife.com, a website parodying Second Life (including its distinctive "eye-in-hand" logo) which might have expected an aggressive "cease and desist" request. But no! Linden Labs chose to rise above it all. It revealed itself to be a champion of "creativity and self-expression" and, rather than objecting, Linden Labs magnanimously granted a license to proceed with use of its modified logo on the site, earning it considerable public kudos in the process.

A bad month for… having an iMoan about the iGasm

Apple was outraged this month over an Ann Summers poster promoting the iGasm. The iGasm plugs into any portable music device, and complements the music by, well…actually, you work it out! The poster for the iGasm replicates Apple's silhouette iPod campaign, and features a person apparently enjoying the iGasm. Apple is refusing to get into the groove and have angrily demanded the immediate removal of the posters. However, Ann Summers suggested in a press release that it would send Apple an iGasm by way of a peace offering and to put smiles on their faces. It is not known whether Apple accepted the offer.

CD WOW spanked for £41m in damages

Online music retailer CD WOW has received a judicial rap over the knuckles to the tune of £41m for breaking the terms of an agreement not to import cheap CDs illegally from Hong Kong into the UK.

The High Court had ruled in March 2007 that the site's owners, Music Trading Online (HK) Limited, had breached its undertakings in a 2004 agreement not to import CDs originating outside Europe into the UK. Current copyright laws permit music companies to charge different prices in different regions, according to market conditions. It is illegal to import CDs into the European Economic Area (without consent) with the aim of selling them on at a cut-price to consumers, a practice known as parallel importing.

CD WOW, seizing the moral high ground as "the little guy" fighting the good fight on behalf of music-lovers everywhere, claimed that it was a "coincidence" that test purchases by the claimant were parallel imports, easily explainable as "human error". Unsurprisingly, the High Court was unmoved. There was strong evidence to suggest CD WOW was committing a widespread breach of its 2004 undertakings, and had not taken effective steps to remedy this.

UK IP rights holders will find reassurance in the outcome. The decision, and the scale of damages awarded, serves as a cautionary tale for overseas traders targeting UK consumers online. It also highlights the importance of obtaining positive test purchases as evidence in establishing that copyright infringement (or in this case a breach of undertakings) has taken place.

Champagne producers fail to obtain champagne.co.uk

Entrepreneur Steve Jackson raised a glass to toast a decision this month permitting him to hold on to the domain name champagne.co.uk. However, the celebrations were short-lived when the decision was overturned three months later on appeal.

Jackson had registered the domain name in 1997. The Comité Interprofessionel du Vin de Champagne (CIVC), representing producers in the Champagne region of France, issued a complaint to Nominet's DRS service, albeit 10 years later. CIVC argued that Jackson's initial registration of the domain name in 1997 was abusive, and took advantage of the goodwill associated with the "champagne" name. Until the date of the complaint, Jackson's use of the site had been primarily for non champagne-related purposes, including links to his website selling car number plates.

The original expert acknowledged CIVC's rights in the name but held that these were the result of Champagne's protected region status within France, and did not equate to trade mark rights in the name. Jackson's use of the name was not seen to be abusive by the expert.

In August, however, CIVC succeeded in its appeal against the expert's refusal to transfer the domain name. The appeal panel found that the registration was abusive because of Jackson's use of the domain name to link to commercial websites, including his own websites. As users would visit his website expecting it to have some connection with "Champagne", he was taking advantage of "initial interest confusion" to attract visitors to the domain name.

BBFC loses appetite for video game nasties

January

February

March

April

May

June

July

August

September

October

November

December

In June, the British Board of Film Classification (BBFC) took the unusual step of refusing to grant a certificate for a computer game. As a result, Manhunt 2, the PlayStation 2 and Nintendo Wii game, which no doubt cost millions of pounds to develop, cannot legally be sold in the UK.

Only certain video games need a BBFC certificate: those that realistically depict gross violence, human sexual activity or techniques likely to be useful in committing criminal offences. The regime is the same as for films, with releases awarded a U, PG, 12A, 15 or 18 certificate or, as in the case of Manhunt 2, no certificate at all.

The BBFC's powers are taken from the Video Recordings Act 1984. It is a criminal offence to sell a certified computer game to persons below the relevant age group shown on the certificate. If the BBFC refuses to certify a work, it is illegal to supply it to anybody.

The BBFC considers rejecting a work entirely to be a very serious step, and would normally attempt to have games modified to remove offending content rather than refusing to certify them. In relation to Manhunt 2, it did not think that modifying the game in this way would be possible. It stated that the game was '*distinguishable from recent high-end video games by its unremitting bleakness and callousness of tone in an overall game context which constantly encourages visceral killing with exceptionally little alleviation or distancing*.' The BBFC also criticised Manhunt 2's '*sustained and cumulative casual sadism*'.

The BBFC did grant a (18) certificate to the original Manhunt game. But the new game apparently had an 'unrelenting focus on stalking and brutal slaying' and a different overall narrative context. The BBFC stated that Manhunt was already at the very top end of what it considered to be acceptable.

The decision not to certify Manhunt 2 appears to show a shift in what the BBFC considers acceptable in terms of video game content. Indeed, the BBFC has hinted that the original Manhunt game might not have received a certificate were it to be released today. This change in stance is influenced by some research into video games, which the BBFC published in April. David Cooke, director of the BBFC, commented that younger players '*often admit that they find the violence in games like Manhunt very upsetting*' and, although games could be given an 18 certificate, the research indicated that parents '*are happy to give their children adult games because they are "only games*".'

This was the first game to be banned by the BBFC since it refused to grant a certificate for the infamous "Carmageddon" game in 1997. In that case, the BBFC's decision was successfully appealed to the Video Appeal Committee (VAC), which required the BBFC to grant an 18 certificate. In December 2007, the Video Appeals Committee also overturned the BBFC's decision to ban Manhunt 2 (even in a modified, less violent, state). The BBFC applied for judicial review against this decision and was successful in its application. At the time of going to press, the latest position is that the VAC have been ordered to reconsider their position by the Court.

A further article on the legality of "downloadable" video games is included on page 30.

A good month for… eBay shoppers

Shill bidders beware, the US courts are coming after you. A shill bidder (the American term for a 'plant', i.e. someone pretending to be something they are not) is someone who colludes with the seller at an auction (or is the seller) artificially to drive up prices by placing bids on the items. As anyone who has used an online auction site will know, shill bidders are evil, and need to be stopped. In June, an e-bay jewellery seller paid out $400,000 in fines after it was shown to have made 232,000 bids for its own items. The New York Attorney General summed up the result by saying: "Consumers should not have to surf with sharks" (pun, we're sure, intended).

A bad month for… complete and utter idiots

A lesson for all teenage drivers: if you must swerve between lanes at 140mph on the M65 in your dad's Toyota MR2, don't film yourself on your phone and then post the footage on YouTube. Eighteen-year-old Nathan Campbell is learning this the hard way, after a court appearance in June led to a four month jail term and a three year ban from driving. After the sentence was handed down, police condemned Campbell's actions as being of "the utmost stupidity".

In West Philadelphia born and raised

A number of celebrities have won the right to boot cybersquatters off domains that use their names (for example juliaroberts.com). In June, one celebrity went further and forced the transfer of a domain that used not his real name (Willard C. Smith II) but his hip-hop alter ego (the Fresh Prince).

Smith's claim, a WIPO UDRP complaint, was made in respect of the domain name "freshprince.com". To succeed, he needed to show that the domain name was confusingly similar to one of his trade marks, and that the owner of the domain name had no legitimate interest in it and had registered and used it in bad faith.

The tricky part of the claim was that "Fresh Prince" is not a registered trade mark. The panel found, however, that common law trade mark rights existed in the name. As the Fresh Prince, Smith had sold 5 million hip-hop albums and made 146 episodes of the sitcom "the Fresh Prince of Bel Air". The panel also commented on his two Grammy Awards.

The decision suggests that celebrities enjoy fairly wide protection from cybersquatters, covering both their name and alter egos that have obtained sufficient recognition. We don't know whether Smith has any plans to pursue registration of his other moniker, "Big Willie" (nor have we checked to see whether anybody is using the domain name…)!

Reassurance for ISPs in relation to terrorism offences

Internet Service Providers (ISPs) benefit from a number of exemptions from liability under the 2002 E-Commerce Regulations. This covers ISPs where they are acting as hosts or mere-conduits, or where they cache data. However, these exemptions only apply to laws that were passed before the E-Commerce Regulations were implemented in 2002 and do not apply to laws passed since that date.

The Terrorism Act 2006 includes a number of offences for which ISPs could be liable, including encouraging acts of terrorism and disseminating terrorist publications. There is a requirement to take down illegal material from a website when instructed to do so by a police constable, otherwise the ISP can be regarded as having endorsed any illegal statements or conduct. There are some defences available in the Act, but none as far reaching as those offered by the 2002 E-Commerce Regulations to other criminal offences found in earlier legislation.

In June, the government addressed this inconsistency by issuing the Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007. These Regulations create exceptions from liability for offences under the Terrorism Act 2006, including the dissemination of terrorist information, where ISPs act as mere conduits, caches or hosts of information.

However, it was not all good news for ISPs. The 2007 Regulations also extend the "country of origin" principle to the Terrorism Act, meaning that UK ISPs can be liable for the conduct and statements of their users, even if all of an ISP's services are directed to and provided in other European countries and not the UK.

Spanish data protection laws protect peer-to-peer users

January

February

March

April

May

June

July

August

September

October

November

December

The Spanish copyright licensing group for music producers, Promusicae, suffered a blow this month in its ongoing attempts to force Spain's largest Internet service provider (ISP), Telefónica, to reveal the identity of Spanish file-sharers.

Promusicae had identified a large number of file-sharers by their IP address only, and had asked Telefónica to provide personal details (e.g. name and address) about the users of the IP addresses. Telefónica refused, and Promusicae commenced proceedings in the Spanish courts to attempt to obtain an Order requiring Telefónica to provide the personal details.

During the Spanish court proceedings, Telefónica submitted that the Spanish laws on data protection (which implemented EU wide laws) did not allow it to share personal data of its users with third parties unless it was a criminal law matter. In deciding whether to grant the order requested by Promusicae, the Spanish court thought it necessary to ask the European Court of Justice (ECJ) a question about the validity of Spanish law on data protection, and whether it was compatible with EU directives on data protection, e-commerce, copyright, and enforcement.

At the time of going to press, the ECJ has not answered the question. However, the opinion of the court's Advocate General, which is usually followed by the ECJ, was made available this month. The Advocate General's opinion was not made available in English, but a loose translation of the French version is that "*European law allows Member States to prevent personal data, which relates to IP addresses, from being disclosed when this has been requested to pursue copyright infringement claims in civil law.*" Or in other words, it is not a breach of EU law for Member States can make it illegal to disclose personal data where its disclosure relates to civil proceedings only.

If, as it normally does, the ECJ follows the opinion of the Advocate General, the Spanish Court will need to decide, on the facts, whether the Spanish laws on data protection allow the court to order the disclosure of the file-sharers' personal details. However, it would appear unlikely, given the fact the Spanish Court asked the question in the first place, that it considers itself able, under Spanish law, to force Telefónica to disclose the personal data of its users.

The English courts have previously ordered ISPs to disclose personal details of UK file sharers. For example, in 2005 and 2006 the BPI obtained court orders against numerous service providers requiring them to disclose the personal data of their users. However, it does not appear that in those cases the UK service providers opposed the BPI's court applications on data protection grounds. If the ECJ makes its decision as expected, this will increase pressure on UK ISPs to attempt to oppose future court applications for data protection reasons. It would make it more likely that users who have their details disclosed by ISPs will complain that the ISPs have breached the Data Protection Act by releasing the data.

A good month for… real world laws preventing virtual world fun

The owners of the virtual world Second Life have issued new policies on virtual casinos, covering jurisdictions both friendly and hostile to Internet gambling. It is no longer permitted to take part in games which rely on chance or random number generation to determine a winner, or rely on the outcome of real-life organized sporting events; and provide a payout in Linden Dollars (Second Life's virtual currency) or any real-world currency or thing of value. Virtual currencies are becoming increasingly controversial, as more gaming sites use them to attract players.

A bad month for… treating your biggest fans nicely

French police briefly detained a teenage boy who posted an unauthorized translation of the latest Harry Potter book online within days of the release of the English version. The boy had apparently compiled the entire translation himself. He spent a night in jail and faces charges of intellectual property violation. Author J.K. Rowling's lawyers say networks of other illegal Potter translators span the world, seeking to profit from the boy wizard's global appeal, and growing more sophisticated with every new tome. However, the boy did not appear to be seeking commercial gain and his treatment does therefore appear to have been a little heavy handed.

Belgian ISP ordered to filter Internet traffic on its network

Belgian ISP, Scarlet, has appealed against a surprise court ruling forcing it to filter customers' traffic for unlawful file sharing. Scarlet was ordered by a Belgian Court earlier this month to scan peer-to-peer network traffic and block files identified as unauthorised copyrighted material. It was the first time in Europe that an ISP was held responsible for the content of its subscribers' traffic.

Laws deriving from the E-Commerce Directive protect ISPs acting as "mere conduits" from liability for the content of their traffic and prohibit any general obligation to monitor. The Belgian court's ruling challenges the limits of that protection.

Laws emanating from another EU Directive, the Copyright Directive, appear in some circumstances to be incompatible with the E-Commerce Directive by giving copyright owners certain powers over intermediaries whose services are used for piracy, such as gaining court orders against them. The Belgian ISP Association believes that the over-arching defences in the E-Commerce Directive should take precedence over the Copyright Directive.

The Belgian court took the view that there is no contradiction between the two Directives. The court claimed that its injunction does not require Scarlet to 'monitor' its network, distinguishing monitoring from filtering. It said the technical solutions "are limited to blocking or filtering certain information transmitted on the Scarlet network; they do not constitute a general obligation to monitor the network". It also claimed that the mere conduit defence was not lost, saying that it was irrelevant to the case.

There are fears that the ruling could affect other ISP businesses in Belgium and could even prompt a re-evaluation of laws elsewhere in Europe. ISPs (or Belgian ISPs at least) are awaiting the results of the appeal with bated breath.

Data Retention laws passed

UK telecoms companies now have to keep phone call logs for a year under the Data Retention (EC) Regulations, which were published this month but did not come into force until October 2007. The Regulations transpose into UK law most of the EC Data Retention Directive.

The new Regulations are intended to ensure that security services have a reliable log of mobile and fixed-line phone calls to be used in investigations, and relate not to the content of calls but only to records of their occurrence. Such communications data is a vital investigative tool, providing evidence of associations between individuals and placing them in a particular location. Without it, the ability of the police and the security services to investigate the associations between those involved in terrorist attacks would be limited. The Regulations will ensure that the communications data will be available uniformly, regardless of which communication provider supplies the service.

The Regulations do not apply to records of Internet activity, such as web surfing, email and Voice over Internet Protocol phone calls. Many participating in the consultation process felt that the complexity surrounding the Internet made the draft Regulations an inappropriate framework for implementation of the Internet aspects of the Directive as this would present particular technical and resourcing issues. The Directive allowed member states to extend the rules to Internet data at a later date, provided these rules are in force by 15 March 2009.

Royalty rates for digital music downloads and streaming

January

February

March

April

May

June

July

August

September

October

November

December

August saw the UK Copyright Tribunal (the Tribunal) make an interim decision regarding collective copyright licensing, and digital downloading and streaming. The decision centred on how much is paid in royalties when music is used or transferred in an online service. These online services include permanent downloads, limited downloads and on-demand streaming/webcasting.

The British Phonographic Industry (BPI) made the application to the Tribunal together with a number of major Internet companies (including music download sites) and mobile phone companies. The respondents were the collecting societies protecting the proprietary rights of creators and performers (the Alliance).

The decision emanates from a long-running dispute between companies using digital music and societies tasked to collect royalties for performers and composers. The BPI and other distributors applied to the Copyright Tribunal (an independent body established under the Copyright Designs and Patents Act 1988) to settle their dispute. In September 2006, a settlement agreement was made between the Alliance and the majority of the industry parties. The agreement included the new joint online licence. The recent interim decision dealt with outstanding issues that had not been resolved in the agreement and included an endorsement of the terms of the settlement agreement including the licence (which would apply to all rights owners moving forwards).

The decision contains a number of key points, namely that the Tribunal:

- endorsed the settlement agreement, including the new joint online licence;
- agreed that the settlement agreement's joint online licence would form the template for future online licensing;
- endorsed the royalty rates set out in the joint online licence, which are a percentage of revenue as follows: permanent download, 8%; limited download or on demand service, 8%; webcasting where more than half is by a single artist or band, 8%; premium or interactive webcasting, 6.5%; pure webcasting, 6.5%. Downloads to mobile phones were agreed at the above rates less a small discount;
- confirmed the new joint online licence's approach to the concept of minimum royalties for the full range of services. This decision will see royalties being paid to rights holders even when, for example, music is given away for free or at a subsidised price;
- looked at a variety of streams of revenue when reviewing the revenue on which the percentage-royalty should be based. This stemmed from the opposition to the definition in the new joint online licence by a number of applicants. They objected to the possibility that the definition may capture advertising revenue linked to music.

The parties spent more than £12 million in bringing the action – an amount that reflects the desire for certainty in the industry. The decision confirms the general acceptance by the Copyright Tribunal of the new joint online licence as a template. It also gives the online corporate users of music a degree of confidence in the level of royalties that they will be required to pay when selling or giving away music. By confirming and setting benchmarks, the decision will aid legitimate use of the constantly developing and growing digital music market.

A good month for… highlighting the stupidity of some Facebook users…

IT security firm Sophos released the results of a survey designed to test how many users of the social networking website Facebook are willing to divulge personal information that would potentially leave them open to identity theft. Sophos created a bogus account and sent out random friend requests. Worryingly, almost half of the recipients not only accepted, but most also gave Sophos access to personal information such as e-mail, dates of birth, addresses and phone numbers. The test highlights that a large number of users are either unaware of the risks or simply aren't treating their privacy seriously (or, of course, that they are idiots).

A bad month for… the US Navy's architect

The US Navy is to remodel one of its barracks which, from an aerial view, resembles a swastika. The series of four L-shaped buildings constructed in 1967, and now nicknamed 'Hitler's San Diego Bunker', are to have $600k spent on them to "change the walkways, landscaping and rooftop solar panels". Apparently the unsettling resemblance to a swastika was noted at the time of construction, but was dismissed as a problem as it wasn't obvious from the ground. If only they had predicted Google Earth!

Snooker loopy nuts are we

The snooker club operator Rileys Limited has failed in its attempt to obtain the domain name rileys.co.uk through Nominet's Dispute Resolution Service. The respondent to their complaint had registered the domain name in 1999, one year after Rileys was incorporated. The respondent was in the business of registering domain names and, at the same time as registering rileys.co.uk, had made registrations for more than a thousand other domain names which had potential commercial value in the future.

Rileys has trade marks in the word 'Rileys' which meant it was easily able to prove it had rights identical to the domain name, thus succeeding on the first limb of Nominet's Policy. It was unable to prove the second limb however, which requires that the respondent's registration was an Abusive Registration. The application therefore failed in front of the original expert.

Rileys appealed and the Appeal Panel reiterated that an essential component of an Abusive Registration in most cases is that it must be shown that the respondent knew of the complainant and/or its rights at the time of registration. Without this knowledge, it could not be found that the respondent's registration was taking unfair advantage of, or was unfairly detrimental to, the complainant's rights. In this case, the complainant provided no evidence that the respondent had the complainant in mind at the time of the registration. The Panel did find that the respondent was dealing in domain names (i.e. was acquiring domain names likely to be desirable to others in the future), but noted that this was, in itself, a legitimate practice.

Ignore dispute resolution clauses at your peril

This month, the Court of Appeal decided in the case of *Douglas Harper v Interchange Group Ltd* that the claims made should be barred, because the claimant had failed to make use of the dispute resolution mechanism written into the contact between the parties.

In 1996 the claimant sold his computer software business to the defendant as part of an asset sale agreement. The agreement provided for commission to be paid to the claimant on certain future revenues of the business. The claimant wrote to the defendant in 1997 alleging that a high percentage of commission was due to him under the contract. The defendant, not believing this to be the case, responded saying that any dispute should be dealt with according to the contractual dispute resolution mechanism. The defendant then heard nothing of the matter until 2002 when it received from the claimant's solicitors a letter with draft particulars of claim attached. The court held that the claimant should be precluded from recovering the sums claimed because he had failed to invoke the contractual dispute resolution procedure.

The case sends out a clear message to parties who sign contracts containing provision for dispute resolution. To avoid any claim under the contract being barred the parties must strictly adhere to such a clause, even if the clause contains, as it did in this case, restrictive time limitations for raising complaints.

Watch out for the patent ambush!

January

February

March

April

May

June

July

August

September

October

November

December

Standard-setting organisations congregate a number of companies and individuals with the aim of agreeing on a device or product standard. The creation of such an industry standard obviously helps to ensure the compatibility and interoperability of products between multiple vendors. To achieve this aim, such organisations may adopt a variety of structures and decision-making processes, some of which will be formal whilst others will rely on an informal method of cooperation.

A "patent ambush" occurs when, during a standard-setting process, an intellectual property owner fails to disclose its ownership of intellectual property which then subsequently forms part of the new agreed standard. This may be by wilful deception aimed at securing inclusion of patents in an adopted standard or as a result of a simple error.

A Statement of Objections is a formal step available to the European Commission in relation to potential anti-competitive practices concerning the use of a patent ambush. The relevant party is informed in writing of the objections raised against it by the Commission. The party can then reply in writing, setting out all information known to it which is relevant to its defence against the Commission's objections. The party can also request an oral hearing to present its comments if it wishes. The Commission considers the response it has received, and then takes a decision on whether or not the conduct outlined in the Statement of Objections is compatible with the EC Treaty's competition rules.

For more than four years Rambus participated in the Joint Electron Device Engineering Council's (JDEC) standard-setting process for DRAM, a type of memory. Rambus did not disclose the existence of patents or patents-pending relating to the technologies ultimately adopted as part of the JDEC's standard. Once the standard was set, however, Rambus then asserted its patents against other manufacturers. Therefore, any manufacturer wishing to produce a DRAM chip must pay for a licence from Rambus or run the risk of Rambus taking action against it for patent infringement.

On 23 August 2007 the Commission sent Rambus a Statement of Objections alleging an infringement of Article 82 of the EC Treaty (abuse of a dominant position). This alleged breach stems from the unreasonably high royalties, enabled by the alleged patent ambush, charged by Rambus for use of the relevant patents. The Statement of Objections preliminarily concludes that an appropriate remedy for this kind of breach would be that Rambus charge a reasonable and non-discriminatory royalty rate. Standard setting organisations would typically recommend cross licensing should be on a FRAND basis (Fair, Reasonable and Non Discriminatory). There have already been parallel proceedings against Rambus in the US. In August 2006 and February 2007 the Federal Trade Commission (FTC) issued orders whereby it found that Rambus had engaged in illegal monopolisation. The FTC imposed a remedy (in the form of a remedial order) applicable to US patents and foreign patents to the extent that they relate to import or export of relevant products into or from the US. This required Rambus to reduce its licence fees.

This is the first time the Commission has characterised a patent ambush as an abuse of dominance. However, the Commission notes that its approach "*reflects well-established general case law under Article 82*".

A good month for… the 25 year old :-)

The "smiley" - a cunning combination of keystrokes which gave rise to the ubiquitous emoticon – celebrated its 25th birthday this month. That's according to Carnegie Mellon University professor Scott E. Fahlman, who says that at 11:44 am on 19 September 1982, during an electronic bulletin board discussion about "the limits of online humour and how to denote comments meant to be taken lightly", he made the following fateful suggestion: "I propose the following character sequence for joke markers: :-). Read it sideways." LOL!!

A bad month for… poking your ex-wife on FaceBook

A man who joined Facebook to look at his friend's wedding pictures was sent to jail after the site "automatically" sent a friend request message to his estranged wife. The man had previously been told by magistrates to stay away from his wife after bombarding her with phone calls and text messages. The man served seven days of a sentence for breaking his bail conditions, commenting that Facebook's sign-in procedure had confused him and that he had not intended to contact his wife. He commented: "People on Facebook should be careful - this could easily happen to someone else." Presumably, for this to apply, the "someone else" would need already to have a restraining order in place against harassing their ex-wife…

Europe claims the UK botched one third of Data Protection Directive

The European Commission is currently investigating problems with the UK's implementation of the Data Protection Directive's Articles. The Ministry of Justice has rejected the Commission's claims that the Data Protection Act 1998 (DPA) does not properly implement European law, asserting that that the Act is fully compliant.

The articles of the Directive which the Commission alleges have not been correctly implemented are articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 and 28 – just under a third of the Directive's 34 articles.

These articles relate to definitions used in the Directive (e.g. the meaning of personal data), the scope of application to manual files, conditions when sensitive personal data can be processed, fair processing notices, rights granted to data subjects and exemptions from these rights, the ability of individuals to seek a remedy when there is a breach, the liability of organisations for breaches of data protection law, the transfer of personal data outside of the European Union and the powers of the Information Commissioner.

The Commission's investigations are thought to have been provoked by the landmark ruling from 2003, in Michael Durant's dispute with the Financial Services Authority, which served to narrow the scope of information that constitutes personal data under the Data Protection Act.

Microsoft CFI appeal: the outcome

This month, the Court of First Instance (CFI) gave its judgment in Microsoft's appeal against the European Commission's decision to fine Microsoft €497 million for abuse of a dominant position by failing to supply interoperability information to competitors and for bundling Windows Media Player with Windows.

The CFI has essentially upheld the Commission's decision and has not reduced the fine imposed on Microsoft. The CFI did, however, decide that the Commission exceeded its powers by requiring the use of a monitoring trustee to supervise (at Microsoft's expense) Microsoft's compliance with the terms of the Commission decision. The CFI found that the Commission has no authority to compel Microsoft to grant to a monitoring trustee powers which the Commission itself is not authorised to confer on a third party. In relation to the refusal to supply interoperability information, the court did not formally consider the existence of IP rights in the information, but instead proceeded on the assumption that there were IP rights in the communication protocols or the specifications and applied the legal test accordingly.

This long awaited judgment sparked lively debates on a number of issues, including on the extent to which the Commission should be able to regulate and attempt to control free markets.

Software developer defeats "implied term" argument in court

January

February

March

April

May

June

July

August

September

October

November

December

The High Court refused to imply a term in to a software development contract assigning the copyright in the software away from the developer. For certainty, the parties must include express provisions of intellectual property right ownership in the written contract.

In 2005 Meridian International Services Limited (Meridian) was commissioned by GlaxoSmithKline plc (GSK) to provide them with financial forecasting software. Before contractual arrangements were put in place, Meridian ran in to financial difficulties and became unable to pay its employees. Employees Mr Richardson and Mr Aldersley left to set up another company, IP Enterprises (IPE). Mr Richardson and Mr Aldersley arranged to meet with Meridian, whereupon they agreed that IPE would carry out the software development, with Meridian being paid a percentage of the project cost of £200,000 as a "finder's fee".

Following the meeting, Mr Richardson sent Meridian an e-mail containing the discussed and agreed terms, adding, "This is as I understand the situation as we agreed yesterday – if you do not agree please let me know today". There was no mention of intellectual property rights in the e-mail, and Meridian did not reply.

Issues then arose as to which company or person owned the IP in the software. There was no dispute that Mr Aldersley was the sole author of the software's source code, nor that he had written it while working as an independent contractor for IPE. However, Meridian claimed that it should own the copyright.

Meridian claimed that at the meeting that it had been agreed as an express term of the contract that Meridian was awarded the copyright. The court found that Meridian could not establish this. Meridian then claimed that there was an implied term of the contract they had with IPE assigning them copyright.

Robert Ham QC, sitting as a Deputy High Court Judge held that when framing implied terms, courts must not go any further than what is necessary to make the contract function (i.e. what is necessary for business efficacy). The trial lasted 7 days, during which Meridian offered several reasons for the copyright assignment term to be "necessary". These included the fact that the software contained Meridian's confidential information and their need to prevent IPE from reselling the software.

The Court would not imply a term in to the contract that Meridian was entitled to assignment of the intellectual property rights in the software. It was held that confidential content in the software did not lead to the conclusion that there was an implied term as to ownership of copyright (the law of confidence would provide Meridian with protection), and that there was no "necessity" from both parties' point of view for Meridian to prevent IPE from approaching other customers. The High Court found that IPE was the owner of all copyright in the software.

Software developers typically seek to retain copyright and re-use code in subsequent contracts. This case highlights the importance of addressing intellectual property in the contract, particularly in the IT and technology sectors.

A good month for… stopping people from modding games consoles

A UK businessman was convicted for advertising and selling 'modchips' which enabled games console users to play copied games. This was the second conviction of this nature since new offences relating to anti-circumvention devices were brought in to force in 2003. The man had been in business nearly two years when Trading Standards officers from Bristol city council led a raid on a flat belonging to his parents. Nine computers were seized and more than 100,000 files examined for evidence at his trial. It is estimated that his business had £1m in turnover by the time of the raid.

A bad month for… listening to the radio at work

A judge in Scotland refused to dismiss a £200,000 damages claim brought against Kwik-Fit over the use of personal radios in the workplace by Kwik-Fit employees. The Performing Right Society (PRS), which collects royalties for music publishers and songwriters, is claiming that Kwik-Fit is in breach of copyright because it doesn't hold a licence to play music on its premises. Kwik-Fit claim they have had a policy banning use of personal radios for 10 years but they face a tough challenge: PRS claim to have countrywide evidence of 250 occasions of the playing of music by staff which was audible to colleagues and customers from 2005 onwards.

Spam by Bluetooth – now allowed

In a spectacular result for marketers, the ICO reversed its position on the regulation of Bluetooth technology.

Before October, the ICO had included marketing via Bluetooth in its guidance on direct marketing via public electronic communications networks. This meant, amongst other things, that consent was required before marketing messages could be sent to consumer's mobiles. The nature of Bluetooth made this a difficult task; manufacturers often set phones as 'discoverable' in the default settings, preventing consent being inferred from the ability to receive communications; and as Bluetooth involves no concept of 'reply', opt-out systems could not be effected as with SMS and MMS marketing.

Following discussions with other regulatory bodies, the ICO has deemed that Bluetooth escapes the clutches of this consent requirement. It stated that a public electronic communications network means a network provided wholly or mainly for the purpose of making electronic communications services available to members of the public, a definition not consistent with Bluetooth.

The result is that marketers may now target consumers in specific locations via their mobiles, without the burden of SMS and MMS costs. Using Bluetooth mobile technology, marketers may send out instant messages directly to Bluetooth enabled mobile users containing coupons, single-track song downloads and even short video clips (users do have the option of not accepting the downloads).

The ICO anticipating consumer fears that the regulation U-turn would invite a burst of 'BlueSpam' was careful to stress the growing awareness and concern of consumers, and encourages marketers to follow industry guidelines and good market practice when devising marketing strategies. The ASA rules of advertising would continue to apply, for example.

ISPs get new exemptions from religious hatred offences

The Racial and Religious Hatred Act created a number of new religious hatred offences in England & Wales including intentionally using threatening words or behaviour and displaying threatening written materials. One way these new offences might be carried out is through website text, forum posts or blogs. This put ISPs, website operators and search engines at risk of committing an offence under the legislation. For their protection, new Regulations came into force this month which extend the protections available to service providers where they act as mere conduits, caches or hosts of information under the E-Commerce Directive.

While these exemptions have been warmly received in principle, ISPs and website operators must ensure that website terms and conditions and usage policies require that users do not upload material potentially infringing the Racial and Religious Hatred Act.

As mentioned in the articles for June in relation to terrorism offences, ISPs benefit from a number of exemptions from liability under the 2002 E-Commerce Regulations. However, these exemptions only apply to laws that were passed before the E-Commerce Regulations were implemented in 2002 and do not apply to laws passed since that date. As a result, new e-commerce defences must be enacted for each new offence or civil liability created by parliament to ensure that the UK complies with its obligations in the E-Commerce Directive. This has resulted in a piecemeal approach to legislating which could result in dangerous inconsistencies in the law and an uncertain legal framework for ISPs.

First RoHS enforcement action

January

February

March

April

May

June

July

August

September

October

November

December

This month, the National Weights and Measures Laboratory (NWML) confirmed that it had taken its first formal enforcement action since the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Regulations 2006 came into force on 1 July 2006. The RoHS Regulations were introduced to implement the EU Directive on the restriction of the use of hazardous substances in electrical and electronic equipment (2002/95/EC), which prohibits the marketing of new electrical and electronic equipment containing more than prescribed levels of certain hazardous substances (such as lead, cadmium and mercury) in the EU.

Although in this instance the company was not fined for selling electrical equipment containing excessive lead in the UK, it did receive a documented warning, which can support a legal action if the company is found to be in further breach. Additional details have not yet been provided since the level of failure was not considered serious enough to warrant public disclosure. The NWML's actions, however, suggest that it may have cautioned the company following an admission of a breach, and served a compliance notice requiring the company to withdraw, or modify non-RoHS compliant equipment.

The NWML highlighted some compliance issues that are arising in practice in the news release that it released following press reports and interest in the case:

- Most electronic products tested by the NWML are in breach of the RoHS Regulations "but the degrees of failure are small or questionable".
- There are concerns over the competence of company employees to understand the technical information, which indicates whether particular equipment is compliant.
- Where companies run both RoHS and non-RoHS compliant lines in their factories for different global markets problems with cross-contamination are prevalent.
- When outsourcing the production of components it is important to have robust controls to ensure production is RoHS-compliant.

This case is only the second formal RoHS enforcement action that is known to have been brought in the EU, the other having been instigated by the Danish regulatory authorities. The NWML considers that there have been no significant UK enforcement cases to date because industry has generally been cooperative. However, it has stepped up its compliance checks and recently bought off-the-shelf products for testing.

There has been widespread criticism of the RoHS Directive, particularly the additional administrative burdens for industry. he European Commission is proposing to make changes to the RoHS Directive in 2008, including:

- harmonising compliance across the EU to provide a more level playing field for manufacturers
- streamlining the grant of exemptions from the RoHS Directive to manufacturers
- improving enforcement through market surveillance and administrative cooperation.

The NWML's recent enforcement action and increased testing suggest that it is stepping up its enforcement activities. However, it has worked closely with industry to encourage compliance without formal enforcement. Its reluctance to reveal the name of the company in this case suggests that, in practice, this will continue to be its preferred approach.

CMS Cameron McKenna LLP

A good month for… Wikipedia, which succeeded on its e-commerce defences in France

Wikimedia, the owner/operator of Wikipedia, was afforded the same protection enjoyed by ISPs as a French court acknowledged that the company that publishes the encyclopaedia could not be held liable for user contributions. Three men sought €69,000 in damages and the disclosure of the anonymous contributor's identity when a Wikipedia entry identified them as gay activists. The French employee laws exonerated the company and the fact that the articles in question were censored shortly after Wikimedia was informed of the claims was taken into account when acknowledging Wikimedia's role as an Internet host, rather than an editor.

A bad month for… data security – when the details of 25 million people "go missing"

November saw the names, addresses and the dates of birth of every child in the country, and the bank account details and National Insurance numbers of 10 million parents, guardians and carers go missing. Two password protected discs containing a full copy of HMRC's entire data in relation to the payment of child benefit was sent to the National Audit Office by HMRC's internal post system operated by the courier TNT. It seems that the package, which was not recorded or registered, has failed to reach its addressee and is still lost in the (internal) post.

Court Orders website to disclose details of forum posters

The High Court ordered the operator of a football club fan website to disclose the identity of five users of the site in relation to the posting of allegedly defamatory messages concerning the management of Sheffield Wednesday Football Club. However, the court refused to order the disclosure of the identity of nine other users, finding that their messages were of a more trivial nature. In doing so, the court set out some clear guidelines as to when a court can require a website operator to disclose the source of defamatory material by way of a *Norwich Pharmacal* order, which build on the principles previously established.

The case illustrated that a court retains ultimate discretion and will not reach a decision to require disclosure lightly, as it will have an impact upon an individual's right of privacy and freedom of expression. Factors such as the strength of the claimant's case, the gravity of the defamatory allegations, whether it was part of a concerted campaign, and whether the defendant had a confidentiality policy for website users will all be taken into account.

In this case the website operator did not oppose the claimants' application, but he was not prepared to go as far as consenting to it, as he regarded it as inappropriate for him to do so. Although there was no formal confidentiality in place for users, the operator considered that users could reasonably expect that he would not disclose their personal details without a court order. Should the European Court of Justice make its expected decision in the Promusicae case (see the articles for July), this would give more weight to any data protection arguments raised against such disclosure.

Google DoubleClick deal to be investigated on competition grounds

This month, the European Commission announced the launch of an extensive, second-phase review of Google's merger with advertising giant DoubleClick on competition grounds. The regulators will determine whether to let the deal go through as is, to let it pass with modifications, or to veto the merger. As the Commission has 90 days to make a decision on the future of the combined company, its decision must be made before 2 April 2008.

The Commission has stated that:

"[The Commission] will investigate whether the merger, which combines the leading providers of respectively, on the one hand, online advertising space and intermediation services, and, on the other hand, ad serving technology, could lead to anti-competitive restrictions for competitors operating in these markets and thus harm consumers…"

Google obtains the majority of its revenue from the text ads that appear beside the answers to search queries and Doubleclick is an online ad-serving company whose systems post and monitor Internet adverts. The investigation will examine whether, without this transaction, DoubleClick would have grown into an effective competitor of Google in the market for online ad intermediation.

Over the past 10 years the Commission has pushed only about three per cent of its cases into a second-phase review. The vast majority of deals are allowed to go through either as planned or with some modifications, such as a divestiture of a division or subsidiary. It would therefore be an unusual and bold step should the Commission take further action here.

High Court upholds publican's conviction for receiving the foreign broadcast of football

January

February

March

April

May

June

July

August

September

October

November

December

In what must have been a nice Christmas present for BSkyB, the High Court dismissed an appeal by a publican against her conviction for screening a broadcast of live UK Premier League football matches, which she received from a Greek broadcaster. The broadcaster only had the rights to screen such matches in Greece, whereas BSkyB held the UK rights from the Premier League.

The UK's Premier League owns the intellectual property rights relating to the screening of Premier League football matches. The defendant was the landlady of a public house in Southsea, Hampshire. On becoming the licensee, she cancelled her subscription with BSkyB, which has the exclusive licence to screen live Premier League football matches in the UK. She instead paid for equipment that enabled her, for a far smaller sum, to receive broadcasts of live Premier League games from Nova, a Greek television-provider, which was the Premier League's licensee for Greece.

The Premier League brought a private prosecution against Ms Murphy in respect of two Premier League matches screened at her public house. She was convicted of two offences in the Magistrates Court and her first appeal was rejected by the Crown Court.

Ms Murphy appealed against conviction, relying on the following arguments:

- The Nova transmissions she received were not made from a place in the UK, but from Greece, and therefore the requisite Copyright, Designs and Patents Act 1988 (CDPA) provisions had not been satisfied.

- The visual images, sounds or other information produced at the ground and transmitted first to the Premier League, and then onwards to Nova, were not a broadcast satisfying the definition in the CDPA.

- There was no programme to which the words "with intent to avoid payment of any charge applicable to the reception of a programme" could apply, because the programme that she received from Nova was not the same as any other "programme included in a broadcasting service provided from a place in the UK".

The High Court dismissed Ms Murphy's appeal, subject to a further hearing on EC competition law issues.

The question of whether a programme included in a broadcasting service was provided from a place in the UK had to be answered by identifying what was said to be the "programme included in a broadcasting service" and then determining where that broadcasting service was provided from. The fact that this programme had a commentary and Nova's logo added to it did not change the identity of the programme, as received by Ms Murphy.The requisite intent to avoid a charge was proved if it was shown that the defendant knew that the broadcaster had the exclusive right in the UK and charged for the reception of its broadcasts, and that he made arrangements to receive its broadcasts without paying the charge.

If the appeal on EC competition law points is unsuccessful, this case may spark lobbying at the EC level to open up the markets for broadcasting in Europe.

A good month for… VoIP providers who do not give access to emergency services

Ofcom has published a statement setting out its approach to regulating access to the emergency services from Voice over Internet Protocol services (VoIP services). VoIP service providers allow users to make voice calls through their computer via a broadband connection. Ofcom had concerns that consumers are confused about whether they can call 999/112 from VoIP services. Its statement requires most providers, except "Click to Call" services (i.e. buttons on websites which connect customers immediately to customer service agents via VoIP), to provide 999/112 access at no charge. This is an update to Ofcom's previous position on this subject (see the articles for April).

A bad month for… saying things were NOT made in China

An OHIM Board of Appeal has rejected applications to register the expression NOT MADE IN CHINA as a word mark and as a figurative mark resembling a postage stamp, on the ground that this phrase, whether with or without a graphical element, could operate as a direct and unambiguous description of the geographical origin of goods (that was, that they had been produced in a country other than China). The decision highlights the principle that, where a term may be interpreted fancifully (as here, a tongue-in-cheek declaration of high quality) or as a literal description, the existence of the literal meaning is enough to prevent registration of that term as a trade mark, even if the public are unlikely to take it at face value.

Crown Prosecution Service issues guidance for prosecutors under Computer Misuse Act

The Crown Prosecution Service has issued guidance on the factors to be taken into account by prosecutors when considering a prosecution under the Computer Misuse Act 1990 (the CMA) relating to the supply of articles used to test and/or audit hardware or software. The guidance states that there is a legitimate industry in these dual-use articles concerned with the security of computer systems. Prosecutors need to ascertain that the suspect has a criminal intent.

The relevant factors are as follows:

- Did the company or other body have in place robust and up-to-date terms and conditions or acceptable use policies?
- Were students and customers made aware of the CMA and what was lawful and unlawful?
- Did students and customers have to sign a declaration that they did not intend to contravene the CMA?

In determining the likelihood of an article being used to commit an offence under the CMA, prosecutors should consider the purpose for which the article was developed, its availability, how it is generally used and the context of the offence.

The CPS guidance will, to some extent, be welcomed by those working in the IT security industry, in particular the recommendation that the primary purpose for which an article has been developed should be taken into account on prosecution. However, there is no guarantee that the courts will follow it.

On a practical level, companies and institutions involved in the supply of computer tools should take steps such as updating terms and conditions, and implementing acceptable use policies, as these will help to demonstrate their lack of criminal intent if their products are used for illegitimate purposes.

High Court rules ex-employees infringed database right by copying electronic files

In the case of Crowson Fabrics Ltd v Rider and others, the High Court has held that ex-employees who copied and retained various documents belonging to their ex-employer, such as customer contact details and sales figures, had not acted in breach of confidence, because the information was available in the public domain or from within their gathered skills and expertise.

However, the ex-employees had infringed their ex-employer's database right by copying substantial amounts of customer sales figures and electronic files from its computer system to the computer system of a competing company set up by the ex-employees.

A database right subsists in a database if there has been "*... a substantial investment in obtaining, verifying or presenting the contents of the database*". The maker of a database (who must be based in a European Economic Area state) is the first owner of the database right in it. The "maker" is the person who takes the initiative in obtaining, verifying or presenting the contents of a database and assumes the risk of investing in it. A database right is infringed if a person extracts or re-utilises all or a substantial part of the contents of the database without the owner's permission.

This case illustrates the potential utility of relying on database right in cases where ex-employees have copied and retained information after termination of their employment without permission.

Article 1

Developments in Open Source – 2007

2007 has proved to be a busy year in the world of free and open source.

January saw the European Union's approval of version 1 of the European Union Public Licence (EUPL), the first open source licence to be released by an international governing body. The EUPL is intended to be used for the distribution of software developed within the framework of the IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) programme. It is tailored to EU law and to conform to the existing copyright laws of each of the EU's member states.

A further event of note was the intervention by the Freedom Task Force, part of the Free Software Foundation Europe (FSF) over BT's Home Hub, a network device that uses the Linux kernel, that is subject to the GNU General Public License (GPL) version 2 (GPLv2). The FSF challenged BT's distribution of the Home Hub without the firmware source code as required by the GPLv2. BT admitted that the Home Hub used Linux kernel version 2.6.8.1 but argued that it also used proprietary software which it claimed was not subject to the GPL. Following notification by the FSF that it was acting in breach of the GPL, BT published source code for certain parts of the firmware. The FSF continued to argue that BT has failed to also offer the scripts needed to compile the code, but no further action appears to have been taken against BT.

The release of version 3 of the GNU General Public Licence (GPLv3) finally occurred in June following nearly 2 years of public consultation. Developments in the world of information technology and software have meant an update was due to GPLv2. Highlights of the new GPLv3 licence include the following:

- "Tivoisation" refers to the distribution of free software in a device which cannot execute modified versions and has the effect of curtailing the right to modify software. The GPLv3 prevents tivoisation in respect of devices whose primary application is not industrial by requiring distributors of such products subject to the GPLv3 to provide whatever information or data is necessary to install modified software on the device.
- Legal controls on circumvention of "effective Technological Protection Method" were introduced in various jurisdictions through adoption of the 1996 WIPO Copyright Treaty which renders the removal of copy protection (without requiring copying or distribution) a violation of copyright. The GPLv3 incorporates a declaration by the licensor that no code distributed under it shall be an "effective Technological Protection Method". Accordingly, no licensor can take action against a party modifying code subject to the GPLv3 under the WIPO based legislation.
- The GPLv2 provides that if code subject to its terms is distributed, it must be distributed with no additional restrictions. This requirement extends to any modified versions of the code, including software created from a combination of code subject to the GPL and code subject to a different licence. Many open source licences however contain restrictions that the GPL does not, some of which are not in reality restrictive as they are easily complied with. To address unintentional incompatibilities, the GPL v3 expressly permits the incorporation of certain additional restrictions. A distributor combining code subject to a different licence can accordingly satisfy its responsibilities to the licensors of both codes and distribute without violating either licence.
- The GPLv2 stems clearly from American law. The GPLv3 attempts to sever itself from its origins in American law through the increased use of defined terms (moving

away from terms borrowed from US copyright law) and by permitting licensors to redraft sections of the licence to better cater for local law. The GPLv3 reads more as a piece of legislation than a licence as a result.

- Under the terms of the GPLv2, modification of code subject to the GPLv2 for the purposes of running web services for payment does not amount to "distribution". Developers of such modifications are accordingly not required to publish the source code to these modifications. The GPLv3 addresses this position by incorporating two new requirements. First, anyone who distributes code subject to the GPLv3 and provides a patent licence to some recipients must automatically extend that licence to all recipients. Secondly, the GPLv3 precludes the distribution of code subject to the GPLv3 if an arrangement is entered into with another software distributor that involves the payment of that distributor not to sue one's customers.

Harald Welte (founder of gpl-violations.org, an organisation which identifies and prosecutes GPL violators) brought an action against Skype in the German courts in July. Skype sells the WSKP100 phone which uses the Linux kernel (subject to the GPLv2) on its website and in various countries, including the UK and Germany. In selling the phone, Skype had issued a flyer that contained URLs to the source code, but it did not give every user access to the source code with the handset as the GPLv2 would require. The court found that by not including the binary version of the software, Skype had violated the GPLv2 as the GPLv2 only permits a URL for software that is delivered over the Internet.

In August, SCO's high profile series of suits against IBM and corporate Linux users for alleged misappropriation of its UNIX System V code finally collapsed. SCO's claims were premised on its acquisition of parts of Novell's UNIX business in 1995. On obtaining the UNIX business, SCO began claiming rights to UNIX, issuing a number of suits against, and seeking royalties from, certain GNU and Linux users and distributors. Novell meanwhile claimed that the copyright in UNIX had not been assigned in the sale and began registering the copyrights to certain UNIX products. In August, the federal district court judge in SCO v Novell ruled that Novell, and not SCO, held the copyrights covering the UNIX operating system resulting in the collapse of SCO's claims. SCO filed for Chapter 11 bankruptcy in September.

The first US suit over alleged violations of the GPL was filed in September by the Software Freedom Law Centre (SFLC) on behalf of BusyBox developers Erik Andersen and Rob Landley against Monsoon Multimedia. The suit has been hailed as signalling a new level of assertiveness on the part of open source software developers. BusyBox is a set of standard UNIX utilities commonly used in embedded systems and is open source software licensed under the GPLv2. Monsoon Multimedia allegedly bundled the BusyBox open source application with some of its applications without providing the source code.

The suit against Monsoon Multimedia could have provided invaluable debate and clarification over the legal status of the GPL, namely whether violation amounts to copyright infringement or breach of contract (resolution of which is pivotal to the remedy for violation). Sadly, it was swiftly settled out of court in October.

On behalf of the developers of BusyBox, SFLC commenced another three law suits in November and December against Xterasys, High-Gain Antennas and Verizon, which rounded up the open source tale of 2007. 2008 will yield the results (or settlement) of the SFLC's actions, but the main question for 2008 is whom Harald Welte, the FSF or the SFLC will target next.

Nicolette Phong
nicolette.phong@cms-cmck.com
+44 (0)20 7367 3685

Article 2

Are online video games in a Regulation Free Zone?

In June 2007, the British Board of Film Classification (BBFC) took the relatively unusual step of refusing to grant a certificate for the video game Manhunt 2. Left with little choice, the publishers of the game, Take-Two Interactive Software (owner of Rockstar Games), decided to withdraw the game from sale in the UK while they decided whether or not to appeal the BBFC's decision. The game was also banned in other countries, including, amongst others, Ireland, Italy, Switzerland and Germany.

On the other side of the Atlantic, in the US and Canada, the game was also effectively banned when the Entertainment Software Rating Board (ESRB) awarded it an AO (Adults Only) rating, which is the highest possible rating. However, unlike the decision of the BBFC in the UK, the decision of the ESRB did not make it an offence to supply the game in the US and Canada. Instead, the decision meant that the majority of retailers in the US and Canada would simply refuse to stock the game.

Both the application of criminal law in the UK and the application of a voluntary code of practice in the US and Canada resulted in the release of the game effectively being regulated so that the game was banned.

One platform for which Manhunt 2 was developed is the Nintendo Wii, which provides a download service for its users (only older generation games are offered for download at the moment). Similarly, Microsoft's Xbox Live service allows games and game demos to be downloaded onto Xbox consoles and has more than 7.1 million users. Valve Software, the creator of the Half-Life 2 computer game, operates a download service called 'Steam' for PCs. A recent Valve press release (May 2007) reports that Steam has more than 13 million users, all of whom can purchase and download new games. It would therefore appear to be both technically possible and commercially feasible for Take-Two Interactive Software to offer Manhunt 2 for download rather than to license the game for sale on disc.

This therefore begs the question: to what extent would the game have been regulated if, rather than being offered for sale on a physical data carrier, such as a DVD, the game had been offered for download instead?

BBFC powers

The BBFC's powers in respect of video games are found in the Video Recordings Act 1984 (the Act). The Act applies to all Video Works, the definition of which is very wide and includes "any series of visual images" which are produced electronically by the use of any "device capable of storing data electronically". Normally, video games are exempted from the provisions of the Act (and therefore the remit of the BBFC). However, they are not exempted if, to a significant extent, they depict: (a) human sexual activity; (b) gross violence towards humans or animals; (c) human genital organs or human excretory functions; or (d) techniques likely to be useful in, stimulate or encourage the commission of offences. If a video game is not exempted, it becomes subject to the classification regime contained in the Act as if it was a film.

There are a number of serious criminal offences in the Act. It is an offence to supply, offer to supply, or possess with an intention to supply, a not-exempted uncertified

game. This carries a maximum penalty of an unlimited fine and imprisonment for up to two years. It is also an offence to supply a game to a person below the age specified in the classification awarded by the BBFC (e.g. U, PG, 12, 15, or 18). The maximum penalty for this is a £5,000 fine and imprisonment for up to six months.

The Act was created when access to high-speed Internet connections was limited and, therefore, at a time when it was not technically feasible to download video games of the type which required classification. As a result, the wording of the Act is not clear as to whether or not it applies to downloaded games and there are no court decisions on point. However, although the Act will apply to video games that are sold on the Internet (e.g. via an online retailer) and which are delivered on disc, the wording would appear not to apply to video games which are offered for download.

The definition of "supply" in the Act is very wide and includes any manner of supply. However, the definition of "video recording", to which the sections in the Act containing the offences all refer, is: any disc, magnetic tape "or any other device capable of storing data electronically". The Act therefore requires that a "device" be supplied, rather than just the video game. It is therefore unlikely that the Act applies to video games that are offered for download only.

There are other criminal laws in the UK which apply to the content of video games. For example, video games which incite hatred may be subject to the Public Order Act 1986, and games which contain obscene images may be subject to the Obscene Publications Acts 1959 and 1964. However, none of the other criminal laws requires that video games are classified or provide for a public body to review the video games and to regulate or to provide guidance on their content.

Unless and until the Act is amended, it would therefore appear that the publishers of Manhunt 2 would be able to offer the (unclassified) game for download in the UK without committing an offence.

"...the publishers of Manhunt 2 would be able to offer the (unclassified) game for download in the UK without committing an offence."

The fact that video games offered for download appear to be unregulated has led to some games publishers selling video games on disc which have been classified by the BBFC, but offering special downloads for the game which later affect their content. The new game (with new content unlocked or added by the download) may not have been given the classification awarded by the BBFC or, in some situations, it may not have been classified at all. The best known example of this is the "hot-coffee" modification for the Grand Theft Auto: San Andreas game, for which a simple download revealed a sex-themed mini-game within the full game.

ESRB and PEGI

The ESRB in the US and Canada, and the Pan European Game Information (PEGI) in Europe, both operate voluntary schemes to which video game creators, publishers, and retailers are all encouraged to join. Both organisations have a code of practice which regulates the conduct of members and the ESRB also has binding terms and conditions which it states it can enforce against its members to ensure that the code of practice is complied with. Both classify games with an age and content rating system designed to inform parents and others about the content of video games before they are purchased.

Neither the ESRB or PEGI has the ability to ban a video game or to criminalise its distribution. However, retailers which are members of the schemes, which will include the majority of large retailers, will enforce the content ratings given and may refuse to stock games which have not been given a rating. In the US and Canada, an Adults Only (AO) rating will effectively result in a video game being commercially unsuccessful

because the majority of large retailers (such as Wal-Mart) will refuse to sell the game. European retailers appear happy to sell 18+ rated games, although the higher age rating may affect sales of the video game.

Both the ESRB and PEGI will provide a rating for any game submitted to it by one of its members, and a video game that is intended to be distributed online can be submitted for a rating. In July this year, PEGI announced a new rating for online games. Games publishers will be able to add a new "PEGI Online" logo to their promotional material for a game if they have signed up to PEGI's online safety code and framework contract. This includes an obligation to keep the website "*free from illegal and offensive content created by users and any undesirable links, as well as measures for the protection of young people and their privacy when engaging in online gameplay.*" There is also an obligation only to include content in the online game which has received a rating from PEGI.

Many websites which offer games for download (e.g. Microsoft's MSN site) will only offer games which have received an ESRB and/or PEGI rating. Similarly, Microsoft, Nintendo and Sony, the three key players in the games console industry will not allow a video game to be downloaded over their proprietary download services unless it has received an ESRB or PEGI rating. A similar culture of industry self-enforcement is therefore developing in relation to online video games, particularly in relation to video games for games consoles; if the game is not rated, the large download sites may refuse to offer the game for download. However, this may only have a limited effect on video games released for a PC, because the games' publisher could easily offer the game for download on its own website.

Conclusion

In the UK at least, online games and video games offered for download do not appear to be subject to any legally enforceable regulation. The games will be subject to criminal laws which apply to all downloadable content, such as the laws relating to the distribution of obscene images, but there appears to be no requirement to submit downloadable ultra violent or games featuring sexual content for classification. Industry bodies operating the voluntary codes of practice may have the power to regulate and potentially prevent the release of online games for games consoles, but it may be some time before that power spreads to affect the distribution of online games for PCs.

"In the UK at least, online games and video games offered for download do not appear to be subject to any legally enforceable regulation."

Phillip Carnell
phillip.carnell@cms-cmck.com
+44 (0)20 7367 2430

This article was first published in the September 2007 edition of E-Commerce Law and Policy,

Article 3

The Audiovisual Media Services Directive

Following lengthy negotiations, the Audiovisual Media Services Directive (AVMS) was enacted on 19 December 2007. The Directive amends the TV Without Frontiers Directive (TVWF) and Member States have 2 years to transpose its provisions into national law. The adaptation of the TVWF Directive takes account of the changes in communication technologies and financing to create a new level playing field in Europe for emerging audiovisual media services.

The AVMS Directive has been the source of significant controversy due to its extension from traditional broadcast networks to all "audiovisual media services". These services will consist of commercial services, where "*the principal purpose of which is the provision of programmes in order to inform, entertain or educate, to the general public by electronic communications networks*" and audiovisual commercial communications, which will be advertising images included in a programme in return for payment or similar consideration or for self-promotional purposes.

The definition of "programme" means that radio broadcasts will not be caught, but anything which can be likened to TV broadcasting is likely to fall within the definition. It will cover, for example, IPTV, mobile TV, webcasting and video on demand. Any audiovisual content which is incidental to the service and not its principal purpose is excluded from the scope. This will therefore leave online-games, private emails, search engines, blogs and other user generated content outside the scope of the Directive. Also excluded from the scope of the Directive are activities which are primarily non-economic (i.e. personal websites).

The Directive distinguishes between a) **linear services** i.e. TV broadcasts (scheduled broadcasting via traditional TV, the Internet, or mobile phones, which "pushes" content to viewers) and b) **non-linear services** i.e. video on demand services (viewing at the moment chosen by the user on the basis of the service provider's catalogue, which the viewer "pulls" from a network). This distinction responds to industry concern that the technical practicalities and financial impact of complying with heavier regulation will drive these smaller enterprises, which provide emerging technology services, outside of Europe. It also reflects differences in user choice and control.

The **linear** broadcasting rules will be in a modernised, more flexible form than the current regulation. The Directive relaxes the rules on the insertion of advertising in TV programmes and the daily advertising limits (although the hourly limits will remain), as well as being open to new forms of advertising (such as split-screen, virtual or interactive advertising). The right of reply, which allows a response to be broadcast where, for example, the reputation of a company has been damaged by the assertion of incorrect facts, will continue to be applicable only to television broadcasts.

The **non-linear** services will be subject only to a basic set of minimum safeguarding principles, e.g. to protect minors and prevent incitement to racial hatred.

Examples of the key rules for all (both linear and non-linear) audiovisual media services include that:

- the identification of the media service provider (MSP) must be clear at all times

- they must not contain any incitement to hatred based on race, sex, religion or nationality

- advertisements must not be surreptitious or use subliminal techniques. Similar rules to those currently applied by the CAP codes on alcohol, advertising to children, tobacco, medicine etc will also apply. The Directive also expressly states that Member States and the Commission must encourage MSPs to develop codes of conduct which will ban the advertising of junk food to children

- sponsorship rules – Sponsorship will be permitted, provided that it does not affect editorial independence of the MSP and it does not directly encourage purchases. It must identify the sponsorship at the beginning, during and/or the end of the programme. News and current affairs programmes are not allowed to be sponsored, and no programmes may be sponsored by certain products such as tobacco or prescription medicines

- product placement – In Europe, unclear and disparate rules on product placement have so far prevented audiovisual content producers from making use of this important source of financing. While the general rule under the Directive is that product placement is prohibited, Member States may choose to permit it in films, sports programmes and light entertainment, or where there is no payment involved. It is not permitted in children's programmes. There are similar rules to those mentioned above under the sponsorship rules which apply equally to product placement. In addition, warnings must be screened at the beginning and end of the programme and after every advertising break.

The "country of origin" principle, which ensures that only one Member State has jurisdiction over any MSP, has been the cornerstone of the TVWF Directive. It provides MSPs with legal certainty that they need only comply with the legislation of the country where they are established (i.e. rather than 27 different national laws). This rule has previously been, and may continue to be, open to abuse. In an attempt to counter this problem, derogation from the country of origin principle is permitted in some limited circumstances e.g. public security, public health or the protection of children and the fight against any incitement to hatred based on race, sex, religion or nationality.

"...the Directive will have a major impact on MSPs, broadcasters, producers, advertisers and sponsors."

The Directive encourages self and co-regulatory regimes. Ofcom, the Department for Culture, Media and Sport (DCMS) and the Department for Business, Enterprise and Regulatory Reform (BERR) are looking to restructure and amend the codes of practice of existing self-regulatory bodies. In particular, the Association for Television On Demand, the existing on-demand television self-regulator, will be turned into a co-regulatory body with Ofcom. It is predicted that Ofcom will favour a "light touch" in order to encourage innovation and growth of new media. Some secondary legislation is also likely to be required for implementation of the rules relating to the on-demand services.

When implemented by Member States, the Directive will have a major impact on MSPs, broadcasters, producers, advertisers and sponsors.

Susie Carr
susie.carr@cms-cmck.com
+44 (0)20 7367 2551

Technology – expertise

CMS Cameron McKenna is a truly client focused law firm. We understand the unique needs and challenges which face clients in specialist industries, and we strive to provide a service which is tailored to the particular concerns and requirements of each of our clients. Our Technology, Media and Telecoms (TMT) industry focus group is a key hallmark of the firm and we are recognised as a leading practice both in the UK and across Europe. We have experience of the full range of legal issues affecting any major TMT project, transaction or dispute, including in the following specialist areas:

- Advertising clearance and disputes
- Data protection and privacy
- Databases
- Dispute Resolution and litigation
- Domain name registration and disputes
- E-Commerce
- Facilities management
- Freedom of information
- Hardware procurement
- Hardware supply and maintenance
- Intellectual property
- Outsourcing
- Parallel trade
- Regulatory issues, including RoHS
- Reputation issues, including defamation
- Software copyright and patents
- Software development
- Software licensing and support
- Systems integration
- Telecoms and Ofcom regulation
- Website development.

To discuss any technology, media or telecoms issue facing you or your business, please contact us. Our contact details are shown on page 3.

Law-Now™

CMS Cameron McKenna's free on-line information service

Receive expert commentary and analysis on key legal issues affecting your business. Register for free email alerts and access the full Law-Now archive at **www.law-now.com**

CMS Cameron McKenna LLP
Mitre House
160 Aldersgate Street
London EC1A 4DD

T: +44 (0)20 7367 3000
F: +44 (0)20 7367 2000