

C/M/S/

Technology Annual Review

A month by month review of selected
technology legal news from 2008

January 2009



Contents

January	4
February	6
March	8
April	10
May	12
June	14
July	16
August	18
September	20
October	22
November	24
December	26
Article 1: Google Adwords get SPICY	28
Article 2: It's not easy being Green	30
Article 3: Peer-to-peer downloading in the spotlight	33
Our services	39

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: age ratings; CCTV rules; domain names; search engine keywords; software patents; myspace.co.uk; LinkedIn; Facebook; unfair commercial practices; new gTLDs; the Freedom of Information Act and much, much more.

At the back of the Review, we have included three detailed articles on legal issues relating to Google's Adwords, green technology, and the regulation of peer-to-peer filesharing.

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. Our contact details are provided below:



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



Susan Barty, Partner
susan.barty@cms-cmck.com
+44 (0)20 7367 2542



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



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



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



Chris Watson, Partner
chris.watson@cms-cmck.com
+44 (0)20 7367 3701



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

Supplying hackers – now an offence

January

February

March

April

May

June

July

August

September

October

November

December

In January 2008, the Crown Prosecution Service (CPS) issued guidance on the factors prosecutors should take into account when considering a prosecution under section 3A of the Computer Misuse Act 1990 (CMA). Section 3A was added to the CMA by the Police and Justice Act 2006, which came into force on 1 October 2008. This makes it an offence to supply, make or obtain articles in the belief they will be used in CMA offences (e.g. hacking) and was designed to deal with those who produce, for example, articles designed to modify set top boxes or software to hack into computers.

When the new law was passed, the IT industry complained that the offence was too wide. There was a particular concern that the CMA would now criminalise not only the supply of such articles for illegal purposes but also the supply for legitimate security purposes. To allay such concerns prior to the coming into force of the Act, the CPS guidance recognised that there is a legitimate industry concerned with the security of computer systems that generate articles to test and/or audit hardware and software. It noted that articles can have a dual use and that prosecutors need to ascertain that the supplier of such articles had a criminal intent before prosecuting.

The CPS guidance gave the following factors to be considered by prosecutors dealing with dual use articles when deciding whether to prosecute:

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

As the section 3A offence deals with articles that are “likely” to be used for an offence but does not define what the word “likely” means, the guidance gave some indication as to how to interpret its meaning. In construing what is “likely”, prosecutors should look at the functionality of the article and what, if any, thought the supplier gave to who would use it.

In determining the likelihood of an article being used to commit a criminal offence, the guidance stated that prosecutors should consider the following:

- Has the article been developed primarily, deliberately and for the sole purpose of committing a CMA offence?
- Was the article available on a wide scale commercial basis and sold through legitimate channels?
- Was the article widely used for legitimate purposes?
- Did it have a substantial installation base?
- What was the context in which the article was used to commit the offence compared with its original intended purpose?

While the CPS guidance was good news to the IT security industry, there remained several concerns. Open source or free software, for example, may not fit the definition of being sold through legitimate channels where it is not sold. In addition, there was no guarantee that prosecutors or the courts would actually follow the guidance, especially as it seemed to interpret the new section 3A more narrowly than it was drafted.

A good month for... Plugging in your computer, turning it on, waiting for it to boot up, double clicking on your VoIP provider's program icon, and then dialling the emergency services

Ofcom has decided to require Voice over Internet Protocol (VoIP) service providers to allow users to access the emergency services. Ofcom considers one of the most important features of traditional telephone services to be that they allow users to call the emergency services using the 999 number (or the EU-wide 112 number). Apparently, Ofcom had concerns that consumers were confused about whether they could dial 999/112 from VoIP services, which could cause delays in contacting the emergency services and result in harm.

A bad month for... Tasting domain names

The practice of "domain tasting" should effectively be ended by proposals in the draft 2008 budget of the Internet Corporation for Assigned Names and Numbers (ICANN), which called for the practice to be prevented by Registrars. Domain tasting is where the five-day grace period in registering domain names is used to test a domain name's profitability. Domain tasting has been an issue for the internet community for some time, with 95% of deleted domain names in January 2007 being accounted for by domain tasters.

BBFC ends its Manhunt witch-hunt (eventually)

In June's articles in last year's Technology Annual Review we reported that the British Board of Film Classification (BBFC) had taken the relatively unusual step of refusing to grant an age-rating certificate for the video game Manhunt 2. This effectively made it illegal to sell the game in shops in the UK.

However, in December 2007 the Video Appeals Committee (VAC) allowed an appeal from Rockstar Games (the developer of Manhunt 2) from the decision of the BBFC, forcing the BBFC to reconsider its action not to grant a certificate for the game.

There was another twist in this saga in January 2008 when, on an application for judicial review by the BBFC, the High Court quashed the VAC's decision, finding it had made an error in law.

It was wrong for the VAC to ask the question "*would the game have a devastating effect on individuals or society if it were released?*" Instead, they should have asked: "*was there a real (as opposed to a fanciful) risk that harm would be caused to potential viewers, including children?*" In other words, it wasn't necessary to show the game definitely would harm people, only that there was a real risk that it might.

The case was returned to the VAC for fresh consideration, which found again that the BBFC should have provided an age certificate for the game. Later in the year, the game was classified with an age rating of 18, meaning that it could legally be sold to those aged 18 or over. The game was finally released by Rockstar Games in the UK on Halloween.

You didn't hear nothing, right...

This month, the Information Commissioner's Office (ICO) published a revised CCTV code of practice (the Code). The ICO has used the Code to make clear its position on CCTV systems that record sound, describing these as "*highly intrusive*" and only ever justified in "*highly exceptional circumstances*". Their own survey had found that seven out of ten people opposed the idea of CCTV cameras being used to record their conversations.

The Code listed several circumstances where sound recording might be justified, including:

- audio-based alert systems (such as those triggered by sudden shouting, as long as the conversations were not recorded)
- two-way audio feeds from help points covered by CCTV cameras (when activated by a person seeking assistance)

- conversations where a reliable recording is needed (such as in a police charging area)
- where recording is triggered by a threat (such as a panic button in a taxi).

The Code is clear that prominent signs, placed where recording may take place, must make it very clear that audio is being recorded.

The Code also laid down more general rules relating to CCTV. Clear and prominent signs should be displayed to let people know whenever there is CCTV recording. Also, where there is a high expectation of privacy (such as in changing rooms or toilets), cameras should only be used to deal with very serious concerns and extra effort must be made to ensure those being recorded know about it.

Additional payments for hardware supplier refused by the court

January

This month, in proceedings brought by Fujitsu Services against EDS, the High Court held that Fujitsu was not entitled to recover additional licensing and system service charges for mainframe computers it supplied to EDS in September 2004.

February

The Department for Work and Pensions (DWP) outsourced its IT services to EDS in 1995. As no business continuity service was in place, EDS established such a service in 1998 by leasing nine Fujitsu mainframes, used to back up the mainframes at the DWP's three other live data centres.

March

In 1999 the parties entered into an umbrella agreement to cover existing and future supplies of computer systems for everyday use. Although further systems could be added under this umbrella agreement, it specifically stated that the business continuity systems provided were excluded from the scope of the umbrella agreement.

April

A further suite of contracts replaced the umbrella agreement in March 2005. However, before the new contractual arrangements were entered into, in September 2004, Fujitsu delivered two mainframe computers to the business continuity centre. These were to be put to everyday use and not business continuity use. No specific charging arrangements were agreed for the new computers.

May

June

Although the mainframe computers fell within the ambit of the umbrella agreement, by mistake (presumably because of their location in the business continuity centre) they were not included on accounting spreadsheets agreed by the parties pursuant to that agreement. They were instead included on a spreadsheet showing charges for the business continuity services, and therefore Fujitsu charged EDS a lower sum than could have been charged under the umbrella agreement. The error was not spotted by anybody at Fujitsu although the spreadsheets were passed round internally for review.

July

August

On review of the agreements, the court found that the express terms included the new mainframe computers as part of the business continuity service (in particular because they were included on agreed spreadsheets). As a result, EDS's claim that there should be no additional charges levied was supported and the judge found that no additional charges were due for the computers in issue for the six months between September 2004 and March 2005.

September

October

The court did consider the possibility that Fujitsu may be entitled to recover the additional charges by virtue of an implied term or *quantum meruit* (a concept of receiving a reasonable value for services). However, as the court found express terms of the various agreements to be applicable, it held that it would be wrong to infer implied terms that contradicted those expressly drafted. Furthermore, the court found that there was no scope for a claim in *quantum meruit* as there was a contractual regime that specifically dealt with the charging for the licensing and system service.

November

December

The case emphasises the importance of clarity when negotiating agreements, in particular the payment terms, and also the importance of following the agreed terms when the agreements are put into operation. This should be the case even where (as was the case here) new contracts are being negotiated or are likely to be entered into in the short term.

A good month for... Texting home from holiday...

Cheaper text messages and downloads are on the horizon in Europe as the European Commission increases the pressure on operators with further threats of regulation. European Regulations in 2007 capped the cost of calls within the European Union (but not texts) and, unless mobile operators voluntarily also reduce text and data charges, the Commission will propose new legislation relating to text messages and downloads. The Commission stated that it did not want further regulation but that it will be forced down that route if operators do not make sufficient reductions.

A bad month for... Violent brain-washed children

Further protection is needed to make the digital world safer for children reports the Byron Review, an independent review carried out by former television psychologist Dr Tanya Byron. In particular, it recommends creating a separate body to oversee a national strategy to keep children safe online and introducing a legally binding DVD-style classification system for video games. To facilitate such a classification system, the review recommends lowering the statutory age at which games have to go before the British Board of Film Classification to 12 (current legislation only provides that games that show sex or gross violence to humans or animals require review by the BBFC).

The European Commission consults on copyright levies (again)

The European Commission announced this month that it had launched another consultation on copyright levies with a view to harmonising the position on levies within the European Union. The Commission had abandoned previous consultations in 2004 and 2006 after deciding that the market was not ready for harmonisation.

The Copyright Directive provides that EU Member States may implement a copyright exception for acts of private copying (e.g. a consumer converting a bought music CD to MP3 files), provided that "rights-holders" receive fair compensation. All EU Member States have implemented a private copying exception except the UK and Ireland. In the UK, the 2006 Gowers Review recommended that a limited private copying exemption be introduced for format-shifting only, although this is yet to appear in new legislation.

To provide fair compensation to rights holders, the majority of Member States

have introduced a system of collecting copyright levies whenever different blank media or copying devices are bought or sold. However, there is no uniformity between Member States with the levies imposed differing in terms of the amount of the levies and the products which trigger the levies.

Issues connected to copyright levies which cause concern, and which the Commission hoped to tackle in the consultation, include cross border trade and e-commerce, issues relating to a "grey market" (e.g. the avoidance of levies due to cross-border trade), the double payment of levies, and the distribution of the levies to rights-holders by Member States.

The Commission is now considering the results of the consultation to decide if a common approach can be found, or mandated, by the Commission.

The Economist fails to obtain the transfer of theeconomist.com

The publisher of the magazine The Economist failed in its attempt to obtain the domain name theeconomist.com after an expert domain name panel at the World Intellectual Property Organisation (WIPO) ruled against the magazine.

The domain name theeconomist.com was registered by Jason Rose in 1996 and only displays a picture of former US chairman of the Federal Reserve Alan Greenspan, with the phrase "*Alan Greenspan, Chairman Federal Reserve Board is THE Economist of the century*". The Economist magazine contacted Jason Rose in 2001 when they first became aware of the domain name but received no response. Another attempt was then made in 2006, this time to purchase the domain name for \$500 but Rose did not accept the offer.

The WIPO panel found in favour of the Registrant, Mr Rose, as it was not possible

to determine that he had been aware of the magazine The Economist when he registered the domain name in 1996. The panel stated that, as the dispute centred on a question of fact (i.e. the Registrant's knowledge), the correct forum to decide such question was a court, where witness evidence could be presented.

For the WIPO panel to have ruled in favour of The Economist magazine it would have had to find that: (a) the domain name, theeconomist.com, was identical or "confusingly similar" to a trademark or service for which The Economist magazine has rights; (b) the Registrant, Mr Rose, did not have rights or legitimate interests in the domain name; and (c) the domain name was registered and used in bad faith by the Registrant. The panel was unable to find (b) or (c) as there was no evidence that the Registrant knew of the magazine in 1996.

Yahoo's hot potato – search engine keywords found not to infringe

January

February

March

April

May

June

July

August

September

October

November

December

In February, the High Court handed down its decision in an important trade mark infringement case brought by Mr Wilson against Yahoo! UK Ltd and its sister company, Overture Services Ltd ("Yahoo!"). The case, which concerned an application for summary judgment and/or strike out, considered whether the use of keywords in sponsored advertising amounted to trade mark infringement by Yahoo!.

Mr Wilson, who represented himself in the proceedings, was a mobile caterer and the proprietor of the Community Trade Mark "MR SPICY". He complained that Yahoo! had infringed his trade mark by selling it to its advertising customers, or 'sponsors', as a keyword in their sponsored advertising service. In particular, Mr Wilson objected to the fact that members of the public entering the words "Mr Spicy" into Yahoo!'s search text box would be directed to the sponsored online listings for Sainsbury's and Pricegrabber.com.

The key points of the High Court's decision were:

- The trade mark "MR SPICY" was only used by the person(s) who typed "Mr Spicy" into the Yahoo!'s search query box, not Yahoo! or the sponsors.
- Sainsbury's and Pricegrabber.com had bid for the keyword "spicy" and not "Mr Spicy". In fact, no one had bid for the keyword "Mr Spicy". Therefore, even if there had been use by Yahoo!, it was use of the ordinary word "spicy" and not "Mr Spicy". "Spicy" is a common word in the English language, contained in many trade marks.
- Further, even if Yahoo! had used Mr Wilson's trade mark, the court found that Yahoo! was not using the mark as a trade mark, in terms of indicating the origin of the goods.

Although this case clearly provides some interesting analysis of trade mark law in the context of search engines, it is only a summary judgment and, unfortunately, Mr Wilson was not legally represented and therefore some of the most interesting points were not addressed in any detail. The decision is, to an extent, a decision on the facts of the case and does not address the issue of advertisers who bid for other companies' trade marks as keywords.

Possible defences to using a third party's trade mark for a legitimate purpose, such as comparative advertising in good faith or where the website owner is a distributor of the trade-marked goods, were also not considered. Nevertheless this decision will be welcomed by search engines and other online advertising providers.

The Court commented that, because the sponsored links made no reference to Mr Spicy, it was difficult to see how the results on Yahoo! had any adverse impact on Mr Wilson's trade mark rights. It is easy to imagine instances where this fact could be a distinguishing factor if similar cases are brought against advertisers who bid on key words (i.e. rather than the search engines) in the future.

In the midst of conflicting judgments from EU Member States' courts, it remains to be seen how this decision by the English courts will influence any eventual interpretation by the European Court of Justice on this area of trade mark law.

A good month for... Japanese recording companies, when ISPs agree to ban flagrant file sharers

Following similar discussions between ISPs and the music industry in the UK and France, Japan's four Internet Service Provider (ISP) associations have agreed to ban filesharers who continually use the country's most popular filesharing program, WinNY, to make pirate copies of software, music and films. Pressure from the Japanese government and copyright owners has led to Japan's ISPs implementing a system, similar to the "three strikes" system proposed in the UK, whereby they will send their customers warnings requesting that they stop their involvement in copyright-infringing WinNY networks. Where a customer ignores the warnings, the ISPs will disconnect its internet connection either temporarily or permanently.

A bad month for... Google, who can't get their hands on Gmail in Europe

The OHIM Board of Appeal dismissed Google's appeal against German trade mark owner Daniel Giersch's opposition to Google's Community application to register the mark GMAIL for services including telecommunications and electronic mail services. In considering the similarity between the mark GMAIL and Giersch's earlier mark "*G-mail... und die Post geht richtig ab*" (G-mail... and off the post goes), the Board concluded that the common GMAIL element of the two marks gave the same overall visual, phonetic and conceptual impression. The Board held that German consumers would therefore be confused into thinking that the marks shared a common commercial origin.

Domain Name disputes reach record number

It was reported by the World Intellectual Property Organisation (WIPO) this month that the number of domain name disputes it has dealt with has increased by 48% since only 2005. In 2007 alone, WIPO dealt with two thousand complaints, almost a fifth more than in 2006.

Cybersquatting refers to the practice of taking advantage of the goodwill in known brand names by establishing website addresses that are identical or similar to those brand names. The idea behind this is that users will be confused into thinking that the cybersquatter's website belongs to the brand owner. This practice often also takes advantage of users who incorrectly type in a website address and are directed to the website of the cybersquatter instead of the brand owner.

WIPO's adjudication process involves an arbitrator who decides the outcome of the dispute. In 85% of cases, WIPO's Uniform Domain Name Dispute Resolution process results in brand owners reclaiming their domain names from cybersquatters. In the remaining 15% of cases, where complaints fail, a complainant still has the option of then referring the dispute to the courts.

Cybersquatting has rapidly become a significant problem for rights holders. Some famous domain names that were involved in disputes during the previous 12 months include those for Facebook, MySpace, the 2010 World Cup and The Prince's Trust.

High Court allows a software patent previously rejected by the Patent Office

The High Court allowed an appeal brought by Symbian Limited against the Comptroller General of Patents (i.e. the Patent Office), holding that a patent application relating to a computer program that improved the method of accessing a dynamic-link library (DLL) should have been allowed.

The hearing officer at the UK Intellectual Property Office had previously upheld the examiner's decision that the proposed invention should be excluded from patentability due to it consisting solely of a computer program (which, under the Patents Act 1977 and the European Patent Convention, is not considered to be an invention and therefore cannot be patented).

However, the High Court allowed the applicant's appeal, citing the now

infamous *Aerotel* case which established a four-step test for determining the exclusion of an invention from patentability. The fourth step in the test is to ensure that the actual or alleged contribution of the invention is actually technical in nature. The judge decided in this case that the invention passed the technical contribution test established in *Aerotel*. The fact that the invention failed the third step of the *Aerotel* test and was excluded subject matter due to it being a computer program should not have precluded the application of the fourth step which allowed its grant.

The Patent Office stated that it disagreed with this decision and that it would appeal. The results of that appeal, which resulted in a judgment from the Court of Appeal, may be seen in October's articles...

Get out of My Space

January

February

March

April

May

June

July

August

September

October

November

December

This month, Total Web Solutions Limited (TWS), the owners of the domain name myspace.co.uk succeeded on appeal in Nominet UK's Dispute Resolution Service against MySpace Inc, the provider of interactive social networking websites including myspace.com. The decision confirmed TWS's right to retain the myspace.co.uk domain name and overturned the ruling of the original Expert who had held that the myspace.co.uk domain was an "Abusive Registration" by TWS under Nominet's DRS Policy.

The victory, however, was somewhat limited in value, as the appeal panel expressed "grave suspicions" about TWS's use of the domain name and said it was uncertain how the courts would react if MySpace Inc proceeded to litigation. In fact, the panel could see no "use" that the Registrant could make of the domain name that would not infringe the rights of MySpace Inc.

The background of the dispute began in August 1997 when TWS registered the domain name myspace.co.uk and began hosting over 290 microsites providing clients with web space and email addresses. Around July 2004, TWS pointed the domain name to another holding page at bigspace.co.uk in turn providing links to other websites, in order to gain revenue from the resulting traffic. At this time, MySpace Inc had been in business for around one year.

Publicity surrounding MySpace changed in July 2005 when it was purchased by News Corporation for \$580 million. Either just before or after this publicity (which could not be determined), in the summer of 2005, TWS discontinued the connection to bigspace.co.uk and a parking page was set up dedicated to myspace.co.uk providing links to the MySpace social networking site. The links were generated automatically by a standard software package on the basis of search engine results.

In 2007, MySpace Inc submitted a complaint to Nominet on the basis that the domain name was an Abusive Registration and took unfair advantage of or was unfairly detrimental to MySpace Inc's rights. The Expert held that TWS was profiting from sponsored links to the MySpace Inc site as evidenced by the changes TWS made to the domain in the summer of 2005, which were a direct result of MySpace Inc's July 2005 publicity. According to the Nominet DRS expert, TWS would have realised at this time that public confusion could be used to generate greater click through revenue.

By the time of the panel appeal in April 2008, MySpace Inc had over 195 million profiles on its sites and 10 million registered users in the UK. Despite this, the appeal panel disagreed with the findings of the Nominet DRS Expert. The evidence was incomplete and there was no means of knowing that TWS exploited MySpace's publicity in the summer of 2005, even if the timing for the changes did appear suspicious. The Panel was also influenced by the fact that the sponsored links on the myspace.co.uk parking page were automatically generated, varying according to the usage made by users of the search engines. Although the links related more and more to MySpace Inc, after the July 2005 publicity, this was automatic, and not something that TWS controlled. As it could not be proven that TWS had done anything actively to exploit its position, it was entitled to retain the domain. MySpace Inc now has the option of taking the matter to court if it intends to pursue TWS further. .

A good month for... Consumer Pirates... Arrrrr

On 10 April, the European Parliament adopted a report which called on the Commission to rethink the issue of consumer digital piracy. The motion pointed out that "criminalising consumers who are not seeking to make a profit is not the right solution to combat digital piracy." Instead the motion called on consumers to be educated about file-sharing through a programme of awareness raising campaigns. The European Parliament also called on all the stakeholders including telecom operators and ISPs to join forces to seek other solutions to the problems of piracy. The motion is not binding on the Commission but is likely to be influential when it plans its next programme of legislation.

A bad month for... Having to hear: "Hello, hello, what? I'm on a plane. Nah, it's rubbish"

Hot off the press this month was Ofcom's statement that it plans shortly to launch mobile phone communication services on aircraft. Radio equipment for these services was later exempted by Ofcom from a requirement to be licensed under the Wireless Telegraphy Act 2006. Small mobile phone base stations called PICO cells will be installed in aircraft with calls routed via the PICO cell to terrestrial networks using satellite.

Time for Re-Phorm

In April 2008, the Information Commissioner's Office (ICO) published the results of its review of the privacy policies of Phorm Inc, the advertising technology company.

Phorm's Webwise and Open Internet Exchange (OIX) software products monitor ISP data in order to generate targeted profile-based advertising for web-users. These products first became controversial when BT admitted trialling them in 2006 and 2007, without first obtaining internet users' consent. This latest review by the ICO came shortly before a new trial of Phorm software by 10,000 BT broadband users without their consent.

According to the ICO, Phorm had confirmed that it does not have access to any information held by ISPs enabling it to link its anonymised user IDs and profiles to a living individual. Accordingly the ICO expressed the view that Phorm is not processing personal data within the Data Protection Act 1998.

Nevertheless, the ICO made clear that the Privacy and Electronic Communications Regulations 2003 (PECR) would still apply to Phorm's products and that, in the ICO's view, Phorm would need to operate on an opt-in basis to comply with Regulation 7. In addition, the Commissioner indicated that the Phorm products will remain under review and the ICO approach will be strongly influenced by the experiences of users, such as those participating in the April 2008 BT trial.

The ICO's statement does not address all of the (some spurious) objections raised about Phorm, and in particular it does not cover any of the objections raised based on the Regulatory and Investigatory Powers Act 2000 (RIPA). In the meantime, Phorm will need to continue to battle to win the hearts and minds of internet users, the majority of whom appear to consider the Phorm service to be an unwelcome intrusion into their use of the internet.

Commission calls for better regulation to protect children from harmful video games

The European Commission published the results of a survey of the video games industry and measures taken by the Member States to protect children from harmful video games this month.

The Communication highlights that the video games sector is a dynamic one with expected revenue of €7.3 billion by the end of 2008. According to the Commission, the industry has also made substantial progress to protect the interests of children by self-regulation. Twenty member states use the Pan European Games Information system (PEGI), an age rating system developed from 2003 by the industry with EU support. PEGI labels provide age and violence/bad language warnings on software and online video games to enable parents to select appropriate games for their children.

However, the Commission also indicates

that the industry must do more to strengthen and update the PEGI system so that it becomes a genuine pan-European tool. Of the seven member states that do not currently use the PEGI system, two countries (Germany and Lithuania) have specific binding legislation and Malta relies on general legislation. However, four countries (Cyprus, Luxembourg, Romania and Slovenia) currently have no system of regulation in place.

In its Communication, the Commission calls for the following measures: better advertising and communication about PEGI online; integration of PEGI with other Member States' legal systems; and better cooperation on age verification at the point of sale. Finally, the Commission recommends that a Code of Conduct should be drawn up for retailers within two years to tackle the issues surrounding sales of video games to children.

That is so unfair

January

February

March

April

May

June

July

August

September

October

November

December

Prior to 26 May 2008, the UK had no law imposing a concept of fairness in business to consumer transactions – but this has now changed since the EC Unfair Commercial Practices Directive was implemented by the Consumer Protection from Unfair Trading Regulations 2008 (CPRs), massively changing the consumer protection laws in the UK.

The CPRs aim to protect consumers from a variety of unfair commercial practices and capture these under a general prohibition, specific prohibitions against misleading and aggressive practices, and a thundering blacklist of 31 practices that will be considered unfair in all circumstances. These will apply before, during and after a contract is made in all business-to-consumer transactions.

Commercial practices will be deemed to be unfair if they fail to meet a standard of honest market practice and significantly impair a consumer's decision-making, causing them to make a decision that they would otherwise not have made.

A misleading practice is one that causes or is likely to cause the consumer to make a different decision. As such, advertising false information about the characteristics of a product, or attempting to deceive the consumer by marketing a product to confuse the consumer with a competitor's product, would constitute misleading actions. Conversely, a misleading omission would occur when a trader omits or conceals important information or provides such information in an unclear or ambiguous manner or does not reveal that they have a commercial intent in the transaction.

Also banned are aggressive practices, considered to be acts that significantly impair the consumer's freedom of choice, through harassment, coercion or undue influence. Finally, the absolute prohibitions that will always be deemed unfair cover, among other things, pyramid promotion schemes, 'bait and switch', whereby consumers are invited to buy a particular product then persuaded to buy a different one, falsely stating that a product will only be available for a short period of time to induce the consumer to make an immediate decision, and using 'advertorials', or an editorial comment to advertise a product, without stating that the trader has paid for the promotion.

The latter, in particular, will impact on blogs, online journals, and web-based retailers, as it will prohibit businesses from providing positive reviews or public ratings of their own goods or services (known as 'flogging') without making their identity clear.

Enforcement of the CPRs is to range from informal regulatory procedures to civil action by industry bodies, and will reach criminal proceedings in the more extreme cases. Complaints will also be likely to be referred to specialised regulatory bodies who would deal with them under their own codes of practice, such as the Advertising Standards Authority which oversees the content of advertisements, promotions and direct marketing in the UK. However, it seems unlikely for now that the new Regulations will fully prevent the occurrence of fake business blogs or spam emails, other than for high-profile cases which will affect a large number of consumers.

A good month for... Sky and Virgin Media, when two men were sent to prison for dishing out information about how to modify set top boxes

'Hairy Monster', 'H', 'Novice Angle' and 'Bubba's Boy' hardly seem to be names that would be used by prison-worthy individuals (not until they are in prison anyway). Yet, hiding behind those aliases, were two men moderating a site called modshack.co.uk, which advised readers how to bypass security settings on their set-top boxes. Virgin Media and BSkyB alleged that the pair helped others to get free services, and by doing so they were defrauded. The two men were charged with providing a hacking advisory service in breach of section 296ZB of the Copyright, Designs and Patents Act 1988, and received sentences of five and ten months in prison.

A bad month for... People over the age of 36...

This month Faceparty took the ageist step of deleting the accounts of all users over the age of 36. The operators of the site claim the step was taken in an effort to reduce the chances of sex offenders navigating the site (because all paedophiles are older than 36, obviously). The professed reason: the Criminal Justice and Immigration Act 2008 contains provisions for email addresses to be checked against a government-provided list for sex offenders, which Faceparty has not done. However, those provisions are not yet operative, nor do they suggest that those over 36 years are more likely to be sex offenders than others.

Cheeky internet site argues that UK law allows the live transmission of UK television online, without a licence

Zattoo.com, operating from Switzerland, was caught re-broadcasting all five UK terrestrial channels online this month. However, it publicly maintained that its actions were not unlawful. The internet service claims to have agreed the rights to rebroadcast 190 channels from eight countries; it profits through broadcasting adverts whenever television users change channels. However, it has not agreed any rights to broadcast UK TV channels and claims that it does not require permission to do so.

Because Zattoo only re-broadcasts live TV as it occurs, rather than archiving programmes, it claims this allows it to benefit from a loophole in UK copyright legislation permitting live re-broadcast from public service broadcasters. The offending section 73 of the Copyright, Designs and Patents Act 1988 concerns the immediate re-transmission by cable of wireless broadcasts and specifies that, subject to certain conditions, copyright in

a broadcast will not be breached if the broadcast is made for reception in the area to which it is re-transmitted by cable.

Zattoo could argue that its activities fall within the loophole, since online delivery could be considered to be re-transmission by cable, and could then restrict its services so that only UK users can view broadcasts made for the UK. However, this loophole has never been tested in court and doing so would be a risky business, particularly for a service operating outside of the UK. The section was originally drafted to cover local retransmission in private dwellings and larger building complexes (e.g. hospitals).

The BBC, Channel 4 and Five state that they have not entered into any licence arrangements with Zattoo, and, along with US networks who sell them material, are unlikely to be content to allow the internet service to continue without a careful scrutiny of the claimed loophole.

Data protection amendments – new punishments and new defences

The Criminal Justice and Immigration Act 2008 was given Royal Assent on 8 May 2008, with its provisions indirectly providing the Information Commissioner's Office with new powers. These included the power to issue penalty notices and fines to data controllers who seriously breach any of the data protection principles set out in the Data Protection Act 1998 (DPA) if the breach is likely to cause substantial damage or distress and the data controller had the necessary knowledge or intention as to his acts. However, the 2008 Act does not provide an indication of fines, which are yet to be fixed by statutory instrument.

As well as this new penalty, the 2008 Act confers power on the Home Secretary to increase penalties for offences under section 55 of the DPA, relating to unlawful

obtaining of personal data. Maximum penalties are presently 12 months' imprisonment and a fine on summary conviction, and an unlimited fine and two years' imprisonment on indictment.

The new Act also introduces a new specific defence for persons breaching the DPA for journalistic, artistic or literary purposes, as long as such persons reasonably believed that they were acting in the public interest.

The new provisions are expected to provide a more effective regime of enforcement for the DPA. However, their success as a new system to enforce data security will depend largely on the levels of new fines and the actual enforcement action taken by the Information Commissioner's Office.

Encouraging employees to use social networking websites: risk versus reward

January

February

March

April

May

June

July

August

September

October

November

December

An application before the High Court this month focused on the tension between businesses encouraging employees to use social networking websites for professional reasons and later restraining the release of confidential information by those employees at the end of their employment. The decision is of interest to employers concerned about the strength of their confidentiality agreements and their policies on the use of social networking websites at work.

The employee in this case, Mr Ions, worked for Hays Specialist Recruitment for six and a half years, initially as a recruitment consultant and subsequently as a managing consultant. Mr Ions then decided to establish his own recruitment business in direct competition with Hays, which he made no secret of before leaving. Mr Ions' contract of employment with Hays included a clause that he was not to "make use of, or disclose or divulge" to any person or company confidential "trade secrets, business methods or information", unless necessary properly to carry out his duties. Mr Ions was also subject to a six month non-solicitation clause.

It was accepted by Mr Ions that he had uploaded the addresses of business contacts onto the professional networking site LinkedIn whilst employed by Hays, although he denied that: (a) the information uploaded was confidential; (b) he had unlawfully used it in his competing business; or (c) he had breached any restrictive covenants in respect of it. Mr Ions specifically argued that the migrating of business contact details to his LinkedIn network was done with Hays' consent, and that the site was a business tool similarly used by his colleagues.

Hays argued that the limited evidence available - evidence that it hoped to supplement through pre-action disclosure - demonstrated that Mr Ions was actively taking steps to gather confidential contact details whilst still employed with Hays, both uploading these details onto his personal LinkedIn network and encouraging Hays' clients and contacts to join him on the site.

The High Court determined that, although there was little evidence which would enable it to weigh up the relative merits of the substantive arguments on both sides, it was satisfied that Hays had an arguable case against Mr Ions. The Court therefore ordered Mr Ions to disclose documents evidencing the business contacts he had uploaded to the LinkedIn website from his Hays computer.

It is notable in the judgment that there was no mention of Hays having a relevant internet use policy. It is not clear whether Hays simply did not have one or whether there was nothing in Mr Ions' conduct which could be said to have contravened it. If there was a policy but it allowed the use of social networking sites, this is evidence of how indispensable they have become to certain companies and their employees.

The key issue in this case is the question: at what point does confidential information of a business cease to become confidential? If an employee is allowed to share contact details of clients on a social network, does the information lose the quality of confidence as soon as it has been made accessible to other contacts? The nature of confidential information and the manner in which the law protects it sits uncomfortably with the nature and purpose of social networking sites.

A good month for... stopping idiots advertising their babies for sale on eBay

Authorities in southern Germany took a seven-month-old boy into care after his parents offered him for sale on eBay "as a joke". The advert used the words "Offering my nearly new baby for sale, as it has gotten too loud. It is a male baby, nearly 28in (70cm) long and can be used either in a baby carrier or a stroller" and had a starting price of one euro. eBay deleted the listing but assisted police in tracking down the parents/complete and utter idiots responsible.

A bad month for... Bloggers' freedom of speech

It was revealed by researchers this month that growing numbers of bloggers around the world face arrest. Since 2003, a total of 64 internet writers have been jailed, most in China, Egypt and Iran. The report, published by Washington University in the US, revealed that more than 50 countries around the world used monitoring and internet filtering to 'watch' posts made on blogs and to review their content. The report predicted that the number of blogger arrests would rise rather than fall.

Update on implied terms in software development agreements

Last year's Technology Annual Review reported on an October 2007 High Court decision which refused to imply a term into a software development contract assigning the copyright in the software away from the developer. This month, the Court of Appeal confirmed that decision and further highlighted the value of determining the ownership of IP rights in software at the outset of a commercial relationship.

The claimant in the case (*Meridian International Services v Richardson*) argued on appeal that the court should imply terms transferring ownership of the copyright to them because such terms were "necessary for the contract's business efficacy and/or so obvious as to go without saying". Meridian claimed that although the High Court had discounted each of its arguments in

relation to necessity and business efficacy, it had failed to consider the cumulative effect of all of the arguments.

The Court of Appeal disallowed the appeal and agreed with the judgment of the High Court, namely that Meridian's arguments only considered 'necessity' and business efficacy from the point of view of Meridian, and not all parties to the contract.

Software developers typically seek to retain copyright and re-use code in subsequent contracts. As a result, the courts have historically found it difficult to imply terms into contracts which assign copyright in software. This is partly because it is unlikely that a software developer would ever have intended such an assignment at the time of contract.

Virgin Media and the BPI start their campaign against filesharers

Virgin Media launched its BPI sponsored/provoked/mandated campaign against illegal downloading this month. Virgin Media customers that are identified (via their IP address) as carrying out illegal music sharing by the BPI will receive two letters: one from the BPI and one from Virgin Media. BPI investigators will monitor the IP addresses of those carrying out copyright-infringing filesharing (e.g. via BitTorrent) and will pass Virgin Media details of the IP addresses in order to identify the customers.

The move is being billed by the Virgin Media as an "education campaign" as, at this stage at least, customers who continue to fileshare illegally will not be disconnected. Virgin Media stated that it will be responsible for distributing both letters, and that no personal information of the user will be disclosed to the BPI.

The Virgin Media campaign is similar to but less extreme than the scheme adopted by Japanese ISPs in March 2008: If a Japanese internet user is warned three times by its ISP about illegal filesharing (i.e. after the recording companies have informed the ISP of the filesharing), then the ISP cuts off the user from being able to access the internet.

This month it was also established that the Japanese agreement would form the basis of new legislation being considered in France. The proposed law, known as the "loi Hadopi" would shift the responsibility for taking action against filesharers onto ISPs and, if implemented, would be the first legislation anywhere in the world to do so.

A Facebook Firsh

January

February

March

April

May

June

July

August

September

October

November

December

Hot on the heels of the *LinkedIn* decision in June, another social networking site received some attention from the courts in July. In the first libel and privacy case relating to Facebook, companies defamed on social networking sites were given hope of a remedy through the courts.

Firsh discovered the profile of himself on Facebook in July 2007. It contained private information and purported to include his sexual orientation and political and religious views, and linked to a Facebook Group, "*Has Mathew Firsh lied to you?*" This held defamatory material, including allegations that Mr Firsh owed his former school friend Grant Raphael "*a lot of money*" and that he had "*constantly lied*" about when he would pay this back.

The profile was created on a computer with the IP address of Mr Raphael, whom Mr Firsh proceeded to sue for libel and misuse of private information.

Facebook took the offending material down at Mr Firsh's request two days after he discovered it, but the pages were live for more than two weeks in total.

Deputy Judge Richard Parkes QC rejected Mr Raphael's claim that the pages must have been created without his knowledge by gatecrashers at a party at his home as 'utterly implausible' and 'far-fetched'. The defendant, he said, was 'glib and loquacious' and the defence 'built on lies'.

Mr Firsh was awarded damages of £15,000 for libel, which included an amount for aggravated damages. The Judge took into account the fact that Mr Raphael continued lying at trial, even though Mr Firsh was willing to accept an apology. In addition, even though there was evidence that only four other people had seen the defamatory material, it had been easily accessible online for 16 days, and the Judge said press coverage of the trial made it even more important to 'nail the lie'.

Mr Firsh was also awarded ordinary damages of £2,000 for misuse of private information. The Judge accepted he was a very private person who was 'shocked and extremely upset' to see his personal details and false details about his sexuality 'laid bare for all to see'. The sum was not higher because aggravated damages were factored into the sum awarded for the libel.

Mr Firsh's company, Applause Store Productions, was awarded £5,000 for the consequential meaning that the company could not be trusted and represented a credit risk due to Mr Firsh's alleged conduct.

This case highlights how easy it is for mud-slingers to create false profiles on free social networking sites if joining requires no verification of addresses or credit card details, but it also confirms that companies that have been defamed on social networking sites, blogs and review sites will be able to recover damages as a result.

A final word of warning, however, victory in such cases will not always be so straightforward: in this case, the defendant was easily identified because he created the profile from his home. If he had disguised his IP address, used a public computer or lived abroad, it would have been much harder to find and to take action against him.

A good month for... Apple

An unlikely white knight came to Apple's rescue when it was saved a major re-pricing and marketing exercise by...the Euro exchange rate. It costs 79p to download a song from iTunes in the UK, but 0.99 Euros in Europe. In January, 0.99 Euros equalled 74p, so Apple promised to standardise prices, ending a European Commission investigation that had been sparked by complaints of price discrimination. In July, the company announced it had delivered on its promise without needing to change any prices, because the value of 0.99 Euros had risen to 79p. It is unclear what Apple intends to do now the exchange rate has changed so that it is cheaper to buy music in the UK.

A bad month for... the Edinburgh Festival "farce"

Ticket sales at the Edinburgh Fringe Festival fell by 10% in 2008 thanks to the collapse of its new online/electronic box office system. The £300,000 system broke down on the first day tickets went on sale for the world's biggest arts festival. The organisers' web support company developed a replacement system, but failed to notice this was unable to print tickets. By the time the original system was working again, there was such a backlog in ticket printing that organisers were forced to ask new customers to come back later. The firm that designed the software, Pivotal Integration, subsequently went into administration.

Original pirate materials

The Government twisted ISPs' arms a little tighter on the issue of policing internet piracy when it launched a consultation on the enforcement framework to combat P2P (peer-to-peer) file sharing.

The consultation acknowledged that ISPs have proved less keen than previously hoped to sign voluntary agreements to help combat such file sharing (the solution suggested by previous reports such as the 2006 Gowers Review). Generally, ISPs are reluctant to give out customers' personal information for this, not only because of contractual and data protection obligations, but also from the not unreasonable fear of alienating their own customers.

The consultation proposed a 'co-regulatory approach' in which ISPs and rights holders would agree codes of practice. These would then be approved

by Ofcom, which would also oversee any self-regulatory mechanism.

In case the ISPs were in any doubt about the Government's vision for their imminent new role, it threw in a few alternative proposals likely to make them even more worried, such as legislation requiring ISPs to divulge their users' personal information or to take action against individual users.

In the same month, the six biggest UK ISPs signed a voluntary Memorandum of Understanding with the Government and music and film industries to combat illegal file sharing. In this, the ISPs agreed to write to customers identified as downloading material illegally. However, the message was undermined by reports that one of the ISPs, Carphone Warehouse, had said the letters would be for notification only and distanced itself from any agreement on enforcement strategies.

Domain name disputes shake-up

Nominet made it easier and cheaper to use its dispute resolution service this month when it introduced a cut-price summary decision procedure as one of several amendments to the service.

Nominet administers '.uk' domain names and the DRS for all disputes relating to these domains. Its decisions are binding on complainants and respondents.

Under the new DRS, if no response is made to a complaint, the complainant can ask an expert for a summary decision (costing £200 plus VAT), rather than going to mediation and paying for a full decision (£750 plus VAT).

Complainants previously had to pay for the full decision even if the other side failed to respond.

Another amendment to the DRS affects the policy on abusive registrations, which was revised to include a "*likelihood of*

confusion" factor. This now says a registration may be proved to have been abusive if the respondent has threatened to use a domain name in a way likely to confuse people into thinking the name is connected with the complainant. This brought the policy in line with English law and a number of the previous decisions of Nominet experts.

Nominet also recognised that some registrations should not be deemed to be abusive purely based on the nature of the person registering the domain name – such as holding a large number of domain names and trading in domain names for profit. The new DRS states that decisions in such cases should be based on specific circumstances and not biased towards any particular result.

The new policy also acknowledges that 'rights' could exist in descriptive terms that had acquired a secondary meaning.

Open market for new Top Level Domains on the horizon

January

This month, brand owners were told they may have to bid in auctions for the right to use new generic top-level domain names (gTLDs) when the new gTLD registration system is shaken up in 2009.

February

ICANN (the Internet Corporation for Assigned Names and Numbers), which manages and allocates all gTLDs, made the announcement hot on the heels of its revelation in June that it had decided to relax its notoriously strict rules on the allocation of gTLDs in favour of allowing people to apply for domain names ending in their chosen words.

March

Currently, web addresses either end in country codes (such as .uk) or gTLDs such as .com or .org. When ICANN announced the shake-up in June, there were just 21 gTLDs.

April

The decision to relax the rules followed 18 months of stakeholder consultation and was prompted by a report by ICANN's Generic Names Supporting Organisation (GNSO) which confirmed in October 2007 there were no technical obstacles to increasing the number of gTLDs.

May

ICANN said it expected applicants to want to use their brand names or personal names in the new gTLDs, as well as names representing communities and said groups have already formed in some cities to bid for city top-level domains such as .paris.

June

The new system is being predicted to have a dramatic impact on how the net is used in Asia, Russia and the Middle East, because the new address system will allow non-Roman letters for the first time. ICANN president and CEO Dr Paul Twomey said: *"There are 1.5 billion Internet users and many non-English speakers will have the opportunity to express the whole of a domain name in characters that look like their language."*

July

The new application system will be a mixed blessing for trade mark holders: on the one hand, it offers the opportunity to apply for gTLDs which include their brand names, but on the other, it offers their competitors and potential infringers the chance to do the same.

August

ICANN said it will not automatically reject applications for words which are trade marks. Instead, if a rights holder spots a proposed gTLD which uses its trade mark, it will need to object and enter a dispute-resolution process with the applicant.

September

In October, the practical aspects of the auction system were put out to consultation when ICANN released a draft gTLD Applicant Guidebook.

October

This suggested that *"rights holders"* (likely to include trade mark owners) would have grounds for objecting to new gTLDs, but did not propose a way of notifying them if an applicant requests a name featuring a registered trade mark. Brand owners will therefore need to monitor ICANN's website carefully for potentially infringing applications to avoid costly court action after a new gTLD is approved.

November

The Guidebook estimated the fee for applications would be around US\$185,000 per applicant, although ICANN admitted it might collect either too much or too little in the first round. If too much, it promised to consult on how to allocate the excess. The Guidebook consultation was due to close in December, with the first round of new gTLD applications is planned for spring 2009.

December

A good month for... Feeling sorry for a Daily Mail journalist

An unsuspecting Daily Mail journalist found herself on the receiving end of an internet campaign this month. Julie Moulton wrote a story in the Daily Mail in which she wrongly suggested that a fake image of Hazel Blears was the top Google search result as a result of 'Googlebombing', caused when numerous fake websites are created to link to another website using a particular phrase to force the website up Google's rankings. To show Moulton that search results can change without 'Googlebombing' occurring, a blogger posted an article and photo entitled "Julie Moulton is an idiot", inviting others to link to it and create similar pages. The inevitable happened and within hours, and to this day, "Julie Moulton is an idiot" is the first search result on Google when the journalist's name is searched for.

A bad month for... The Rich. Idiots. And Rich Idiots.

Apple upset the world's playboys – and one enterprising program developer – when it stopped the sale of a \$1,000 iPhone application called 'I Am Rich'.

The application went on sale at Apple's Application Store for the maximum \$999.99, despite doing little more than displaying an image of a glowing red jewel. In extravagant defiance of the worsening economic climate, eight customers rushed to purchase the application in the 24 hours it was on sale before Apple removed it. But not all were as rich as their extravagance suggested: one reviewer of the product explained: "we jokingly clicked 'buy' thinking it was a joke, to see what would happen. THIS IS NO JOKE".

IPO to supersize copyright fines

The Intellectual Property Office (IPO) suggested giving magistrates the power to fine copyright infringers up to £50,000 this month, as part of a consultation on shaking up copyright protection.

The IPO consultation put forward two options for change:

1. introduce a statutory maximum penalty of £50,000 for copyright offences under the Copyright, Designs and Patents Act 1988 (CDPA); or
2. introduce the same penalty for all IP offences, not just copyright.

The proposals were made in response to a Department for Culture, Media and Sport (DCMS) report in February on protecting IP rights. This recommended consulting on the use of much larger penalties in exceptional cases.

Currently, copyright infringers being tried on summary charges (i.e. by magistrates) can be fined up to the statutory

maximum of £5,000 in a magistrates court in England or Wales. The fine if tried on indictment is unlimited.

Rights owners may welcome these proposals but may also be disappointed that the consultation failed to look into the recommendation of the 2006 Gowers Review of IP. This had said that said penalties for copyright infringement online and those in the 'real world' should be standardised.

Under the CDPA, offences tending to come from 'real world' copying may result in 10 years' incarceration, whereas online offences are subject to a maximum two years. The Proceeds of Crime Act 2002 (POCA) also allows for seizure of all of a 'real world' infringer's income for six years if they cannot legitimately account for it, but no similar option is available for online infringements.

The consultation closed in October with its results to be published early in 2009.

Record-breaking award ordered for file sharing infringement

In a case the software, music and film industries will be very excited about, this month Isabella Barwinska was told to pay more than £16,000 to video games developer Topware Interactive for the unlawful sharing of the game Dream Pinball 3D over a 'peer-to-peer' (P2P) network online. The award, made by the Patents County Court in London, was made up of damages of £6,086.56 and costs and disbursements of £10,000.

P2P file-sharing is the unauthorised sharing of material as music, video games, and film with others using file-sharing programs over the internet. It is estimated to cost the music, games and film industries huge amounts in lost revenue every year.

The judgment was not published. However, it was reported that Barwinska was just one of 500 suspected file-sharers contacted on Topware's behalf and given the option of paying a settlement figure of several hundred pounds rather than go to court. Topware has announced that it is planning to launch hundreds of further cases against suspected infringers of the game.

Some commentators hailed the judgment as setting a precedent that could open the floodgates for prosecutions of P2P file-sharers. However, such predictions are likely to be premature. Barwinska apparently failed to enter a defence or attend the court hearing and the decision of the Patents County Court has no precedential value.

Copyright licensing bodies face competition test

January

In September, the Advocate General confirmed that the Swedish copyright management body could be abusing its dominant position by charging different fees to public and private TV companies for using music. The opinion was largely followed by the ECJ in December.

February

Two Swedish commercial TV channels had complained to the Swedish competition authority that STIM, which collects royalties on behalf of music writers and publishers in Sweden, had an excessive and discriminatory fee model which abused its dominant market position under Article 82 of the EC Treaty.

March

The broadcasters' problem was that STIM charges TV channels for music use in three different ways:

April

(1) The claimants (commercial TV channels) are charged a proportion of their revenue from broadcasts that the music is used in, based on advertising and subscription revenues. This is calculated at the end of each year, based on how long works were transmitted for.

May

(2) Small TV channels are charged minimal amounts, based on how long musical works are broadcast.

June

(3) The Swedish public broadcaster pays fees based on a proportion of theoretical revenues, calculated annually based on an estimate at the beginning of each year.

July

Two months after the Advocate General's opinion was given in September, the ECJ gave its judgment. It found that STIM did have a dominant position in the Swedish market, although it was clear that it is not an abuse of dominance to collect royalties.

August

In this case, STIM's charging methods were not in themselves abusive. The ECJ found that royalties calculated on the basis of the revenue of TV broadcasts were reasonable but only up to the actual economic value of the services.

September

The remuneration model could become abusive if there was an alternative possible method which allowed the use of music and the number of viewers (i.e. those hearing the music) to be quantified more precisely, but only if that method did not unduly increase the cost of managing the royalty scheme.

October

Regarding the fact STIM charged public and private broadcasters differently, the ECJ said that applying dissimilar conditions to equivalent transactions with different trading parties could be an abuse of dominance. However, it was for the Swedish court to examine whether the claimants had been placed at a disadvantage compared to the public broadcaster, whether the two types of channel were competitors, and whether the different fee schemes could be justified.

November

The judgment is clear that competition law will allow dominant licensing agencies some flexibility in deciding the licensing terms used for the use of copyright works. However, the terms (and revenue model) used, must be fair and must reflect the use made of the copyright works by the licensee.

December

A good month for... Techie-smugness in the White House race

Barack Obama launched a mocking attack on John McCain in an advert capitalising on his rival's admitted technophobia. Drawing on interviews with McCain, the ad warned voters that McCain admitted he "doesn't know how to use a computer" and "can't send an email". In July McCain told the New York Times he relied on his wife and assistants to find websites for him to read, and had never felt the need for email. In contrast, Obama not only uses email, but has accounts with MySpace, Twitter and Facebook. Reports that he spends all day updating his status, playing Scrabulous and uploading and tagging embarrassing photos are unconfirmed.

A bad month for... Capitalising on the fall of Freddie and Fannie

Freddie Mac and Fannie Mae were, until September, a formidable pair of mortgage guarantee giants. When the US government announced it was to nationalise them both on 8 September due to financial problems, this prompted huge levels of trading in New York. However, in the UK, the London Stock Exchange buckled and almost collapsed under their weight – or at least its computer system did. Frustrated traders missed out on almost a full day's worth of deals on what was one of the biggest trading days of the year after the big banks lost their connections to the London exchange. Trading was suspended at 9am after early trading began to rise rapidly, and only fully restored at 4pm, depriving hungry investors of their bites of the cherry.

Talented Britons protected online

The company behind the BRITAIN'S GOT TALENT television format obtained a transfer of the britainsgottalent.co.uk domain name from an abusive registrant this month, when Nominet's Dispute Resolution Service (DRS) independent expert ruled in its favour.

The GOT TALENT format first hit the big time in March 2006 when AMERICA'S GOT TALENT was launched in the US. The respondent registered britainsgottalent.co.uk on 15 September 2006.

It was more than a year before the first series of BRITAIN'S GOT TALENT reached UK screens in June 2007. On 4 July 2007 the respondent began actively using britainsgottalent.co.uk, inviting aspiring performers to display video clips of their auditions and making statements such as: "Latest Britains got talent.co.uk videos." It was also alleged that unauthorised footage from the TV show was shown on the website.

The complainant owned a UK trade mark and goodwill in the GOT TALENT mark,

plus goodwill in the BRITAIN'S GOT TALENT mark, because of the programme's huge success.

The complainant failed to prove on balance that the respondent first registered the name in bad faith. Nominet said it could not reject the respondent's explanation that the idea came from his daughter's experiences with a band and the site provided a showcase for performers to audition online.

However, the expert found the respondent had used the domain name in an abusive way after it began operating in July – significantly, after the programme's first series had commenced showing on television. The expert's decision commented: "there is a clear potential for confusion between the BRITAIN'S GOT TALENT programme and the respondent's website". The domain name was therefore used in a manner which took unfair advantage of the complainant's rights in its trade mark.

Sony profits from court action

Sony was celebrating this month after the Court of Appeal awarded it the full value claimed for thousands of memory cards which had been lost by a careless distributor.

The defendant, Cinram Logistics UK, had been given the task of distributing 17,000 PlayStation 2 memory cards which were destined to be bought by one of Sony's largest customers.

However, someone had other ideas and the cards were stolen while in Cinram's care. Cinram admitted liability for breach of contract, bailment and negligence, but disputed the damages Sony was claiming. Sony wanted damages to reflect the market price it would have sold the games for, but Cinram argued it should only pay the price Sony spent on manufacturing the cards, which was much less.

The Court of Appeal found in Sony's favour, saying that a seller should be able to claim for the market price of its goods if they are lost by a defendant, unless the seller had in fact recovered its profit (such as if the customer had placed a replacement order).

The court commented that the burden should not fall on a claimant to prove that it had not managed to make a replacement sale which would give it the same profit as originally expected. If the defendant wanted to argue that the claimant could have earned the profit in this way, the burden should be on the defendant to prove that the claimant had actually done this, and therefore that the claimant had not suffered a loss of profit.

What constitutes “extraction” for the purposes of database right infringement?

January

This month, the European Court of Justice (ECJ) gave its much-anticipated judgment on what sorts of actions will constitute an infringement of database rights under the EC Database Directive.

February

A German professor directed a project at the University of Freiburg to create a list of significant poems. This was published on the internet as *“The 1100 most important poems in German literature between 1730 and 1900”*. The process of choosing the titles was complex and the project took more than two and a half years to complete. The project costs were paid for by the University.

March

Directmedia Publishing GmbH (“Directmedia”) subsequently sold a CD-ROM entitled *“1000 poems everyone should have”*. Out of these, 856 poems appeared in the list created by the professor, Ulrich Knoop. Directmedia admitted using the University’s list in its research for the CD-ROM, but denied simply copying it. It said it had critically examined the University’s list, and had omitted some poems while adding others.

April

Directmedia was sued by Professor Knoop for copyright infringement and by the University for infringement of its database right under the EC Database Directive.

May

The German courts initially found Directmedia liable on the two counts of copyright infringement and database right infringement. On appeal, the Bundesgerichtshof (German appeal court) referred a question about the nature of prohibited ‘extraction’ under the Directive to the ECJ. The question put to the ECJ was whether the concept of ‘extraction’ requires the physical copying of the elements of one database to another, or whether it could include a transferral following a visual consultation of the database and selection of data based on the personal assessment of the transferor.

June

July

The ECJ decided that the definition of ‘extraction’ in the Directive is not meant to apply solely to the mechanical copying of data (literally copying and pasting the data) without any adaptation. ‘Extraction’, the Court said, could include the transfer of data to another database by reproducing data after an on-screen consultation of the first database and an individual assessment of its data. The practical details of the transfer, such as whether the contents were copied by a technical (e.g. electronic) or manual process, or whether the transferor had critically assessed the data, were irrelevant.

August

September

The ECJ’s decision displays a pragmatic approach aimed squarely at furthering what it sees as the Directive’s purpose of protecting the financial investments made by database creators. The Court’s interpretation of the Directive’s aim, as protecting against the *“unauthorised appropriation of the results of that investment”* by someone who reconstitutes the database or a substantial part of it *“at a fraction of the cost needed to design it independently”*, backs up its previous focus on the financial investment behind databases, as set out in *British Horseracing Board*.

October

November

This new decision makes clear that, in pursuit of this aim, the ECJ will expect national courts to take a broad view when assessing whether activities constitute ‘extraction’ of data. Compilers of databases who draw on other databases in their research should be careful to ensure their practices could not constitute ‘extraction’ in the light of this judgment.

December

A good month for... Decency in space

Virgin Galactic rejected a \$1m offer to allow a pornographic movie to be made aboard its SpaceShipTwo vehicle. The money was offered up front but Virgin refused to take the cash, preferring to keep its new space travel service rumpy-pumpy-free. Virgin has already obtained \$40m in deposits from 280 customers keen to take the two hour flight into outer space. Let's hope none of the passengers intend to join the 62 mile-high club.

A bad month for... Hackers and dossers

This month, the changes to the Computer Misuse Act (CMA) came into force. The changes increase the penalties for hacking, clarify the illegality of recklessly or intentionally launching Denial of Service attacks, and introduce a new 'supply' offence (see January's articles) for the supply of articles used in the other offences. However, the fact that most online crimes are committed from abroad, or at least using robot computers based abroad, means it will continue to be difficult to prosecute the main offenders using UK specific litigation.

Software Patents 1 – the Court of Appeal gets technical

In March's articles, we referred to the *Symbian* High Court action, in which the court held that a patent for a computer program that improved the method of accessing a dynamic-link library (DLL) should have been allowed by the UK Intellectual Property Office. This month, the Court of Appeal agreed with the High Court and, in one fell swoop, significantly increased the possibilities of obtaining software patents in the UK.

The Court of Appeal said that it felt bound to follow the position of the court in *Aerotel*, rather than the differing position of the European Patent Office. However, the Court of Appeal warned against there being a clear rule to determine the question of whether or not a computer program is non-patentable. Instead, the court stated that each case must be determined by reference to its particular facts and features, bearing in mind the guidance given in previous decisions, including *Aerotel*.

The Court of Appeal made it clear that considering whether an invention had a technical effect was still an important test when determining patentability. *Symbian's* invention did make a technical contribution, because the computer containing the program would be a better computer and the instructions in the software solve a technical problem lying within the computer itself. In allowing *Symbian's* patent, the Court of Appeal held that: "*a technical innovation, whether within or outside the computer will normally suffice to ensure patentability.*"

To the extent that an invention reveals a technical contribution, this decision opens the way for the UK IPO to grant patents for a wider class of computer-based inventions than has previously been the case in the UK.

Software Patents 2 – the EPO takes a long hard look at itself

The President of the European Patent Office (EPO), Alison Brimelow, asked the Enlarged Board of Appeal this month to address four questions about the patentability of computer programs in Europe. The first question posed to the Enlarged Board asks the general question of whether a computer program should only be excluded as such if it is explicitly claimed as a computer program. The next three questions address where the line should be drawn on what is excluded from patentability.

The Enlarged Board, the highest authority at the EPO, has therefore (finally) been asked to bring clarity to an area where there is perceived to be inconsistency in the EPO's interpretation of what is excluded from patentability in the European Patent Convention. The UK courts have, thus far,

refused to follow the approach adopted by the EPO (see, for example, the article above) and have placed their own interpretation on the exclusions in the Convention.

A similar request by the UK court to the IPO (to review the issue of the patentability of computer programs) was refused last year, so it is interesting to see the IPO make this request of the Enlarged Board. It has yet to be announced whether the Enlarged Board will agree to answer the IPO's request. If it does, it will need to appoint competent members and it is unlikely that answers will be provided in the next two years at least.

Freedom Of [personal] Information Act

January

February

March

April

May

June

July

August

September

October

November

December

In November, the Information Commissioner's Office (ICO) published new guidance (the Guidance) detailing when personal information can be disclosed under a Freedom of Information request. Under both the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) the public can request access to information held by public authorities. The practical approach in the Guidance will enable public authorities to understand the relationship between freedom of information and the Data Protection Act 1998 (DPA) and is intended to promote good practice in applying the exemption for personal data contained in the FOIA (and equivalent provisions in the EIR).

The Guidance states that although the exemption for personal data under the FOIA is absolute (i.e. does not require the application of the public interest test under the FOIA) except in limited circumstances, information will not be automatically exempt from disclosure simply because it is personal data. There is a balance between the public being able to access official information and the need to protect personal information. The Guidance confirms that freedom of information requires the release of publicly held non-exempt information and wrongly withholding such information will breach the FOIA. However, wrongly releasing an individual's personal data will breach the DPA. In order to ensure compliance with both of these regimes, the exemption must be applied with care. The Guidance therefore provides practical step-by-step advice to assist public authorities in applying the exemption.

The first step detailed is to see if the requested information is (or contains) personal data. The Guidance refers to the definition of personal data contained in the DPA and includes any recorded information in any form 'relating to' an 'identifiable' living individual. The guidance also explains how to deal with an individual's FOIA request for information about himself or herself (even if it includes information about other people). Generally, in such circumstances, the request must be dealt with as a subject access request under the DPA.

If the requested information is (or contains) third party personal data, the next step is for the public authority to consider if the exemption from disclosure of such information applies. Much of the guidance focuses on applying the exemption if disclosure would breach one of the data protection principles. The practical explanations use examples taken from the freedom of information ruling that resulted in the disclosure of details of MPs' expenses. The ICO recognises that generally and even though the FOIA exemption is absolute, this will mean considering whether it is unfair to release the information when balancing the necessary public interest in disclosure against the interests of the individual under the first principle.

The guidance also refers to two alternative 'qualified' exemptions for third party data if formal objections have been made or if subject access exemptions apply, but confirms that such exemptions are rarely used, as it is highly likely that the main third party data exemption (referred to above) or other FOIA exemptions will be easier to apply.

Although the Guidance deals separately with requests for environmental information under the EIR, such requests and the application of equivalent exemptions follow the same structure as a FOIA request.

A good month for... Virgin Media customers – who finally get Lost

In November, Virgin Media dropped its competition law action against Sky after Sky agreed to allow Virgin Media to show its television channels on its cable TV network. The agreement came after Ofcom had found that Sky did not have market dominance for its entertainment channels, only its film and sports channels. Virgin has also agreed licence terms for Sky to show channels controlled by Virgin on Sky's satellite network, namely Living, Living 2, Bravo, Bravo 2, Trouble, Challenge and Virgin 1. The two companies have agreed to carry each other's channels until June 2011 at fixed prices.

A bad month for... Terrorists...

This month the Government announced the launch of free filtering software that enables the restriction of access to websites that could encourage the endorsement of, or participation in, acts of terrorism. The software is aimed at parents, educational establishments and businesses. The launch of the software is the result of engagement with software vendors and internet businesses that provide filtering and parental control software. The Government hopes that the "free" software will be used to guard against the viewing of material that promotes or encourages terrorism.

Misselling still high on Ofcom's agenda

This month, Ofcom secured written undertakings from the mobile phone retailer 'Phones 4U' that commit Phones 4U to change a number of its practices. The undertakings were given after Ofcom had found that Phones 4U engaged in a number of practices which breached consumer protection laws.

After discussions with Ofcom, Phones 4U gave the undertakings under Part 8 of the Enterprise Act 2002. If the undertakings given to Ofcom are breached, Ofcom would have the option of applying to court for an Enforcement Order to prevent Phones 4U from undertaking the relevant action. If the Enforcement Order to be breached, Phones 4U would be in contempt of court and could face a significant fine.

The undertakings agreed by Phones 4U were to:

- change its handset return policy so that it complies with the Sale of Goods Act 1979
- change its 'chequeback' terms and conditions so that they complied with the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regulations 1999.
- change its sales practices so that they comply with misleading advertising legislation, in particular in relation to network coverage, mobile plan characteristics, 'unlimited' usage claims, cancellation rights, and upgrades.

In March 2008, Ofcom revealed that it was introducing a new General Condition, 23, which is designed specifically to address the issue of mobile misselling. If this is breached, it would allow Ofcom to issue fines of up to 10% of turnover.

Internet libel – who read what?

This month, in the *Brady* decision, the High Court prevented evidence about the type and number of persons accessing an article published online from being put before a jury in a defamation trial. This was because it was not possible to infer from this evidence that the information published online had been read by the general public and not just those who were entitled to read it (i.e. in a manner that was privileged).

The action was brought by Mr Brady, the former general secretary of the ASLEF rail union, against the current general secretary over an account of the union's annual conference contained in an article which was published in a hard-copy magazine and online. Brady accepted that the communication with members of the union and some other interested parties was privileged (and for which there was no liability) but that was not the case for all parties seeing the article online or

receiving the hard-copy magazine. The ASLEF website, where the article was published, received more than 650 visits per day during the relevant period.

The Court stated that:

"Without some evidence to justify the inference (for instance, evidence that the ASLEF site and the information contained in it provide an attractive resource for transport enthusiasts generally, rather than simply for members and staff) it seems to me to be no more than pure speculation to infer that an 'outsider' would have read the words complained of."

The court therefore decided that there was not enough evidence that anyone without a connection to the union had read the material online, to allow the jury to be presented with evidence on that issue (for example the number of visits the website had received).

Electronic signatures – the Commission has a cunning plan

January

February

March

April

May

June

July

August

September

October

November

December

In December, the European Commission published an action plan with a view to establishing a comprehensive framework that will support interoperable electronic signatures and electronic identification. The Commission's action comes more than nine years after the adoption of the Electronic Signatures Directive (1999/93/EC) in 1999, which delay has frustrated those working to develop technology in this area. That Directive established, among other things, the legal recognition of electronic signatures and a legal framework to promote their interoperability.

The Directive refers to three types of electronic signature:

- Simple electronic signatures. This has a wide meaning and merely serves to identify the signing person and to authenticate data. There are few requirements for this type of signature, and it can include signing an e-mail message with a person's name or using a PIN-code.
- Advanced electronic signatures (AES). This is a more narrow category of signature and involves the use of encryption technology to sign documents and data, and requires a public and private encryption key.
- Qualified electronic signatures (QES). This defines an advanced electronic signature which is based on a qualified certificate. It must be created by a secure signature-creation device.

The Commission has devised the action plan to put in place a comprehensive framework to develop and support interoperable electronic signatures. In particular, the plan attempts to put in place systems which will increase trust in the use of electronic signatures. The action plan proposes that the recipient of an electronic signature should be able to check the quality of the signature. This is difficult at present because of differences in standards and practices between member states and different service providers.

In order to improve the interoperability of electronic signatures, the action plan identifies the following actions:

- to analyse the cross-border requirements for such signatures;
- to prepare a list of trusted, supervised, qualified certification-service providers;
- to establish common guidelines and guidance for the implementation of electronic signatures; and
- to carry out a feasibility study to investigate whether validation tasks can be provided by a centralised validation service.

The use of electronic signatures has developed at a slower pace than was expected when the Electronic Signatures Directive was adopted. This has been frustrating for businesses and for electronic signature service providers. There remains no mutually accepted or recognised electronic signature within the EU, despite the Directive being in place for nearly 10 years.

The issuance of the action plan is a positive step. However, the timetable for progressing the action plan is spread over a number of years, which suggests that the issue of electronic signatures may take a number of years to resolve yet.

A good month for... Dot telling people about .tel

On 3 December, the new .tel Top Level Domain name launched. The domain name is not like any other domain name, as it will not allow registrants to point the domain to an IP address. Instead, it allows contact information and keywords, stored in the .tel domain name server (DNS), to be called upon when the domain name is used. In the words of Telnic, the operators of the .tel domain name: *"It is a bit like an interactive business card on the Web that you can change and give to anyone so they can reach you"*. The idea being that your .tel domain name is the only contact information you would ever have to share.

A bad month for... DNA databases

The European Court of Human Rights (ECHR) ruled that it is illegal for the UK Government to retain DNA profiles and fingerprints belonging to two men who have never been convicted of a crime. The decision is likely to mean that the more than 570,000 DNA profiles in the National DNA Database belonging to innocent individuals will have to be deleted. Police in England, Wales and Northern Ireland currently have powers to take DNA and fingerprints from everyone they arrest. The (ECHR) unanimously found that the UK's DNA and fingerprint retention policy infringes individuals' rights to privacy.

Google AdWords, the fall-out starts

The article on page 28 of this year's Review refers to Google's decision to allow trade marked terms to be registered as Adwords. In December, Interflora, the flower delivery firm, commenced legal proceedings against Marks and Spencer for bidding on the word 'Interflora' as a search engine keyword. If it proceeds to court, the case will be an important test of how UK trade mark laws apply to the 'invisible use' of trade marks in keyword advertising.

Interflora is also taking action against Flowers Direct Online, which is named as a second defendant. Flowers Direct Online is a flower delivery service operating using the domain name flowersdirect.co.uk.

Marks and Spencer and Flowers Direct Online are accused in the legal proceedings of bidding for the words 'Interflora' and common misspellings such as 'Intaflora' and 'Inter-flora' in Google's AdWords programme. When those terms were searched for, adverts for Marks and Spencer and Flowers Direct appeared as Google 'sponsored links'. Interflora claims that the registration of such terms amounts to trade mark infringement.

Marks and Spencer has not denied that it has registered Interflora trade marks as sponsored links, but has stated this to be normal market practice. A search for 'interflora' at the time of publication continues to bring up adverts for Marks and Spencer and Flowers Direct.

Not on my watch

The Internet Watch Foundation (IWF) took the decision this month to add a Wikipedia entry to a blacklist of internet pages containing child pornography. As a result, many internet users in the UK were unable to access the particular Wikipedia page, nor could they edit any Wikipedia article.

The IWF was set up by the internet industry in the UK. The IWF maintains a blacklist of websites containing potentially illegal images that are hosted outside of the UK. It reports the images to law enforcement agencies in the hosting country and adds the URL to its blacklist which is used by UK ISPs to prevent customers viewing the potentially illegal images.

The image in question appeared on the Wikipedia entry for an album by German rock band Scorpions. The image was from the original album cover for the band's 1976 album 'Virgin Killer', which featured a naked young girl in an erotic pose. It was the first time Wikipedia had been added to an IWF blacklist.

After five days, and many complaints, the IWF buckled under the pressure and removed the image from its blacklist. It did, however, maintain its public view that the image was "potentially illegal". The IWF has been criticised since for failing to stick to its guns and ban the image, which many consider to be illegal even to view in the UK.

Google's AdWords policy change gets Spicy

Google's AdWords service allows paying advertisers to place sponsored links to their websites next to the "natural" search results on Google for any given search term. Advertisers bid on the search terms and Google determines (predominantly based on the amount bid by the advertiser) who is successful.

In May 2008, Google caused a stir by announcing a surprise change to its Adwords Policy in the UK and Ireland: it lifted the restriction on third parties bidding for trade marked terms. What is more, with its "keyword suggestion tool", it began suggesting potential keywords (including trade marks) that advertisers might want to bid on. Previously, trade mark owners could notify Google of their rights and request that no other party be able to sponsor a particular term. The prices of paid search advertising are now predicted to rise significantly.

A recent report by Hitwise found that almost 9/10 searches were for branded terms; showing that people tend to go online to search for a particular brand. By allowing bids on any keywords, including trade marks, competitors will have the opportunity to intercept traffic which was directed at a different brand. Brand owners are now presented with two (unattractive) options: bid the highest to try to ensure that they 'win' their trade marked term or risk competitors doing so.

Trade marks can be hugely valuable assets. It is easy to see the objections to Google allowing third parties to bid on trade marks as keywords. The key question is whether Google, or the advertisers, are using the trade marks in a manner which infringes the trade mark owners' rights.

Within the EU, the most relevant types of trade mark infringement are "*use in the course of trade*" of: (i) an identical trade mark with identical goods/services; (ii) a similar/identical mark for similar/identical goods or services such as to cause confusion; or (iii) a similar/identical mark which takes unfair advantage of or is detrimental to the distinctive character or repute of the mark. The key issue on the question of infringement in respect of the use of keywords will be whether such use of trade marks is 'use' for infringement purposes. For this to be the case, the use of the trade mark must affect the essential function of the trade mark, which is to designate the origin of the goods/services.

Google's policy change came shortly after the UK case of *Wilson v Yahoo!* (see March's articles), in which the claimant took action against Yahoo! for trade mark infringement of his trade mark "MR SPICY". The claim was summarily dismissed for a number of reasons, including that the word 'spicy' was generic, and had been sold as a keyword by Yahoo! as such. The judgment commented that use by a 'search engine' of a trade mark as a keyword would not infringe a registered trade mark because there was no use of the relevant words as a trade mark. The extent to which this decision should be relied upon is not clear: it is a decision of a lower court and is not binding on future decisions; the claimant represented himself; and the term used was not the trade mark MR SPICY, but the generic term 'spicy'.

In an earlier decision of the Court of Appeal, *Reed v Reed*, a claim was brought against a party who had used a competitor's trade mark as a metatag and as a Yahoo!

"It is easy to see the objections to Google allowing third parties to bid on trade marks as keywords."

keyword. In a non-binding part of the judgment, the Court commented: *"It may be that an invisible use of this sort is not use at all for the purposes of this trade mark legislation – the computers who "read" sets of letters merely "look for" patterns of Os and Is – there is no meaning being conveyed to anyone – no "sign"."* This comment, which appears to exonerate invisible use only, would justify Google's prohibition of the use of trade marks in the sponsored link itself (i.e. that trade marks do not appear when an AdWord is searched for), although it does not deal with Google's 'sale' of trade marked terms to advertisers.

As it stands, there is no clear case law in the UK. Brand owners considering action against Google or an advertiser will therefore need to make a calculated assessment of the risk and reward. However, if the registration and/or sale of sponsored keywords affects a trade mark's ability to designate the origin of goods or services, it seems at least possible that the registration of a third party's trade mark as a keyword with a search engine (or allowing such registration) would constitute infringing use of that trade mark.

A claim against the advertiser, rather than Google, would be easier to establish. However, if possible, a claim against Google would be attractive because it would be a one hit solution which would remove the ongoing costs of monitoring and/or the costs of enforcement action against multiple advertisers.

Within Europe, the courts have differed from one jurisdiction to the next in the cases brought against Google in respect of its AdWords policy. The most interesting developments have been in France where, in a case in which Google is appealing an earlier successful judgment brought by Louis Vuitton for trade mark infringement, the highest French court, the Cour de Cassation, has referred several questions to European Court of Justice (ECJ). The questions, submitted in May 2008, include whether Google may be liable for trade mark infringement by allowing the use of trade marked terms as Google Adwords.

It is anticipated that the ECJ will focus on whether the use of the trade mark affects the essential function of the trade mark. The referral by the French court presents a superb opportunity for the ECJ to bring clarity to this area of law and coherence to the diverging European decisions. If the ECJ decision is favourable to brand owners, any UK brand owners will be likely to seek to rely on it. However, if a UK brand owner is being negatively impacted by the policy change, it may not feel able to wait until the ECJ provides its ruling, which may take up to 18 months.

Google has stated that it will monitor the effects of its policy change and has claimed that, if the policy fails to improve experiences for users, then it may change the policy again. No doubt the commercial success of the change (reflected in Google's profit) and liability issues, including the impending decision of the ECJ, will also contribute to Google's decision.

"The referral by the French court presents a superb opportunity for the ECJ to bring clarity to this area of law and coherence to the diverging European decisions."



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



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

It's not easy being green

2008 has been a year that demonstrated the growing importance of 'Green IT'. With increasing public concern about the environment, and regular scrutiny directed towards the IT industry as a major consumer of power, companies in the technology sector have been keen to promote their green agenda.

It is perhaps unsurprising that the IT sector has become a prime target for review: the short lifecycle of IT products, energy inefficiency of data centres, and products containing hazardous substances have all come under close scrutiny from environmental lobbyists and legislative bodies alike. Increasing pressure on the IT sector to act clean and green and respond to environmental issues has resulted in some high-profile campaigns. While legitimate attempts to address clean technology issues deserve to be lauded, it is important to ensure that any advertising or green claim remains truthful, accurate and substantiated.

Industry perspective

Earlier this year, CMS Cameron McKenna undertook a survey of suppliers and procurers of Information Technology and Communications (ITC) goods and services to determine how their businesses are affected by 'green' procurement strategies. The survey results revealed that, while businesses are becoming increasingly sensitive to the need to adopt environmentally aware procurement strategies, only a limited number are actually taking significant practical steps to drive supplier performance, although many expect this to change. Policy makers and industry bodies are increasingly taking a more active role in seeking to change procurement behaviour. This has led to publications such as the sustainability reporting guidelines produced by Global Reporting Initiative, Intellect's 'High Tech: Low Carbon' report, and the recently published EU Code of Conduct on Data Centres.

Unsurprisingly, regulatory change featured significantly amongst the factors that respondents considered to be the greatest drivers toward the uptake of environment-friendly procurement policies. The survey results showed that 64% of respondents stated that there are insufficient standards for measuring the environmental impact of ITC goods and services, and 66% were in favour of regulatory enforcement of environment policies. The lack of comprehensive industry standards and consistent or mandatory eco-labelling currently makes it difficult for businesses to set meaningful contractual baselines, or to monitor supplier performance.

Encouragingly, 57% of respondents said their organisations had tangible or fixed targets for reducing their environmental impact. However, only 22% said their organisation specifically measured the energy consumption of its ITC systems (including data centres). Many stakeholders believed that the establishment and enforcement of appropriate industry standards was essential. The imposition of auditable environmental requirements on ITC suppliers, although having cost implications, would enable consumers and businesses alike to be more discerning when seeking out energy efficient products and contracting for performance improvements.

A number of IT organisations have been working with software vendors to reduce the power consumption of their products, and develop tools to evaluate software performance, including making software 'power aware'. Examples of such developments

“While legitimate attempts to address clean technology issues deserve to be lauded, it is important to ensure that any advertising or green claim remains truthful, accurate and substantiated.”

in the open source arena include the 'tickless idle' feature introduced in Linux which only 'wakes up' the Linux kernel when there is an interrupt or when something is expected to happen, thereby reducing the impact of the power-hungry 'standby mode'.

The industry as a whole came under attack in March when Greenpeace effectively chastised the effects of the computer industry and told it to try harder, after its report into the electronics industry suggested that just three of the products reviewed reached the half-way mark in reducing their environmental impact. Greenpeace also commented that the industry was still failing to put together a "*comprehensive lifecycle approach*," meaning that environmental impact was not being reduced in the early part of a product's lifecycle (namely, the manufacture and design stage) or downstream, in terms of extending the lifespan of products. One question facing companies in relation to product lifecycles, as technology improves so fast, is whether to extend the life of inefficient products or discard them earlier in favour of greener alternatives.

In August, Dell claimed that it had met its target to be a carbon neutral company, and the greenest technology firm on earth. This followed the series of programmes it announced in 2007 to reduce the company's carbon footprint and offset its greenhouse gas emissions by the end of 2008. Dell claims to have achieved this goal by "*implementing an aggressive global energy-efficiency campaign and increasing purchases of green power, verified emission reductions and renewable energy certificates*." Dell also claims that its global HQ campus is now powered by 100% green energy. No doubt such claims will be closely investigated.

In November, IBM focused its efforts on 'greening' its data centres to reduce its total 'energy footprint'. It identified practical steps which organisations can take to address the large amounts of energy used by data centres, as follows:

- measure the annual costs of energy consumption and carbon dioxide emissions against the costs of operating 'green IT' before making new investments.
- identify resources that can be unplugged – as much as 10% of IT resources may not be running a workload that is needed;
- compress information and consolidate servers – enabling compression in databases and email systems can reduce storage required by 30 to 80%, without added cost. If an organisation can reduce the number of servers by half it can have a similar effect on energy consumption.

IBM claimed to have achieved 80% annual energy savings by consolidation. By using instant messaging, web conferencing and other social networking tools instead of travel, the company estimated that it is saving \$113 million per year in employee travel.

With all these practical measures being taken by IT companies to address green issues, companies naturally wish to publicise their efforts to an environmentally-conscious public. However, it is vital to ensure that any green advertising meets the criteria set by the Advertising Standards Authority (ASA) to avoid overstating any green claims and risk damage to a company's credibility.

Beware the greenwash

The IT sector has so far escaped censure from the advertising regulator. However, green advertising by companies in other sectors has been criticised by the ASA, and the principles are applicable by analogy to the IT sector.

An ASA Adjudication in October 2007 held that an advert by Maplin Electronics for a solar-powered mobile phone charger was unjustified in its claim "*...if we all used solar mobile phone chargers, we'd reduce CO2 emissions in the UK and Ireland by 3.65 million*

"...it is vital to ensure that any green advertising meets the criteria set by the Advertising Standards Authority (ASA) to avoid overstating any green claims and risk damage to a company's credibility."

“Avoid sweeping or absolute claims such as ‘environmentally friendly’ or ‘wholly biodegradable’. It is unlikely that you will be able to prove your product has no environmental impact.”

tons a year”. Maplin had not provided adequate substantiation for the figures used in the ad as it relied on a newspaper article which quoted from a report by The Carbon Trust. The claim also relied on consumers choosing to charge the device using sunlight rather than mains electricity, a decision which was not confirmed by any evidence.

By contrast, in July 2008 the ASA did not uphold a complaint against Envirofone.com, a mobile recycling company. Envirofone’s TV advert stated: *“So why not recycle your old phone, you’ll get cash and it’s good for the environment”*. A complaint was made that Envirofone’s claim to recycle old phones was misleading, because they sold some old phones for a profit. The ASA noted the ad did not state that Envirofone did not make a profit on the phones and considered that most viewers were likely to understand that it was a commercial company. The ad merely stated that the phones would be ‘recycled’ and viewers were likely to understand that that included re-using the phones, for example by selling them on to other markets. The ASA therefore concluded that the ad was unlikely to mislead.

In 2007 car manufacturer Lexus was criticised for a misleading advert for a hybrid SUV with the headline phrase *“HIGH PERFORMANCE. LOW EMISSIONS. ZERO GUILT.”* The ASA said that readers were likely to understand from this that the car caused little or no harm to the environment and had low CO2 emissions in comparison with all cars, neither of which was the case. In August 2008, the ASA also held that an advert by Shell was misleading in its use of the word ‘sustainable’ in relation to its energy use. Although ‘sustainable’ is a widely used term, the lack of a universally agreed definition meant that it was likely to be ambiguous and unclear to consumers.

How to speak green

The ASA has produced guidance on how to make ‘green’ claims in advertising without overstepping the mark. The ASA has also noted that the Department for Environment, Food and Rural Affairs (Defra) has issued best practice guidance on environmental claims, which states that green claims should not “be vague or ambiguous, for instance by simply trying to give a good impression about general concern for the environment. Claims should always avoid the vague use of terms such as ‘sustainable’, ‘green’, ‘non-polluting’ and so on”.

The ASA’s specific guidance on environmental claims is as follows:

- Get your facts right. Don’t exaggerate the environmental benefits of your product: advertising claims should be backed up with documentary evidence.
- This is an area where scientific knowledge is developing all the time. Don’t present claims as being universally accepted if the science is inconclusive.
- Don’t use pseudo-science, or terms that will not be generally understood by the readers of your advert.
- Avoid sweeping or absolute claims such as ‘environmentally friendly’ or ‘wholly biodegradable’. It is unlikely that you will be able to prove your product has no environmental impact.

The message to those in the IT sector who want to advertise their green agenda is clear: it is important to be clean and green, but you must also be prepared to justify your claims.



Tom Scourfield
tom.scourfield@cms-cmck.com
+44 (0)20 7367 2707

Peer-to-peer downloading in the spotlight

“ISPs are unwilling to divulge the personal data of their customers, due to contractual obligations, data protection legislation and also because they do not wish to alienate their own customers.”

2008 was an interesting year for the internet and for the development of policy relating to how it should or should not be policed. On the one side of a passionate argument, intellectual property rights holders assert that internet-enabled copyright infringement, such as peer-to-peer (P2P) downloading, is destroying their livelihood, costing them vast sums in lost revenue. On the other side of the debate, Internet Service Providers (ISPs) are reluctant to bear the costs of enforcing other parties' rights and are wary of the commercial and legal risks that policing the internet raises.

It is currently not straightforward for rights holders to enforce their rights. First, rights holders need to identify infringers, and in practice this requires at least a degree of cooperation from ISPs. ISPs currently benefit from protection from liability under the E-Commerce Directive (2000/31/EC) whereby those without knowledge who act as mere conduits, or who cache information, or who provide storage space on servers as hosts, are not legally responsible for illegal file-sharing. Once they have knowledge of illegal activity, they must act expeditiously to remove or to disable access to the information.

ISPs are unwilling to divulge the personal data of their customers, due to contractual obligations, data protection legislation and also because they do not wish to alienate their own customers. ISPs generally are reluctant to take action unless compelled to do so by a court order requiring them to divulge relevant details such as the name and address of a person or a relevant IP address. Even where ISPs do not contest the grant of such an order, the process of obtaining it can be costly.

In response to complaints from copyright owners, Governments worldwide have attempted to find solutions to the problem. Some have attempted to put in place new legislation and others have promoted the use of voluntary schemes. Whichever route has been taken however, a common theme is the active involvement of ISPs to help enforce intellectual property rights.

The UK

The Gowers Review of Intellectual Property, published in 2005, reviewed the state of the intellectual property framework in the UK. It highlighted P2P file-sharing as an area of increasing concern and suggested that a voluntary agreement between ISPs and rights holders would be a solution preferable to legislation. In the second half of 2008, the UK Government signed an agreement with certain stakeholders and consulted on proposals to tackle the problem of illegal P2P file-sharing more widely. At the same time, the European Parliament, European Commission and European Council have been developing draft legislation in this area. This has become a politically important and commercially significant issue, engaging policy makers and generating significant press coverage. Whatever the outcome, it is unlikely to please everyone. The decisions reached in 2009 are likely to shape the nature of the internet in Europe and in the UK for years to come.

P2P technology enables participants to form adhoc networks with other users, each providing bandwidth, storage space and computing power to enable file-sharing. However, the technology is often used to share files which are subject to copyright restrictions that do not permit such sharing. A key feature of P2P software commonly

used in illicit file-sharing, BitTorrent, is that, in order to participate in such a network, a user must offer files for upload at the same time as files are downloaded. This practice is claimed to have a significant negative effect on creative industries, particularly the music industry, costing rights holders and distributors millions of pounds.

Currently rights holders find themselves in the unenviable position of choosing either to ignore online infringements or to pursue them, taking on consequential evidential challenges and the risk of bad press and the associated damage to reputation.

In the case of P2P file-sharing, it is difficult for copyright holders to protect their rights. The problem is that sophisticated file-sharers and the websites that promote file-sharing can make it very difficult for rights holders to identify infringers accurately. Websites and P2P software that facilitate file-sharing often insert random IP addresses into lists of users so as to make it harder for the real file-sharers to be identified, thus making it likely that innocent people may be accused. At a local level, wireless broadband connections can be used by people other than those who pay the bill, either where the connection is not secure or where the security arrangements have been circumvented. As a result, identifying the IP address of an infringer from a P2P website is not, in itself, sufficient to prove that the person who pays the bill for that address is involved in illegal behaviour. Consequently many P2P file-sharers, particularly those with wireless connections, will argue *"it wasn't me"*. Without physically checking the individual's computer's hard drive, it may be difficult for rights holders to refute such an assertion.

Rights holders have had mixed successes enforcing copyright in the UK courts in 2008. In August, Topware Interactive, the computer games manufacturer, obtained a judgment for £6,000 in damages and another £10,000 in costs in an action brought against Isabella Barwinska of London, who was found to have illegally shared a copy of the game 'Dream Pinball 3-D'. At the time, despite Ms Barwinska failing to attend court, the case was heralded in the media as an important victory in the battle against online piracy and generated media attention as the start of a new tough stance by rights holders against P2P file-sharers. However subsequent cases, where rights holders have pursued a number of alleged infringers simultaneously, have generated significant negative publicity against the copyright owners.

In the second half of the year, Atari appointed the law firm Davenport Lyons to pursue illegal file-sharers. Davenport Lyons used particular anti-piracy software provided by Logistep to identify potential infringers. However, despite their efforts and convincing a court to require ISPs to cooperate, the press reported that many innocent people, such as the elderly, were wrongly targeted by seemingly heavy-handed enforcement procedures. The consumer group Which? claims some consumers had been scared into paying compensation for something they say they did not do. In November, Which? wrote to the Solicitors Regulatory Authority accusing Davenport Lyons of *"bullying"* and *"excessive"* behaviour. In response, Davenport Lyons issued a press release to the effect that their actions had been in compliance with the law and that they had been acting on instructions.

ISPs are reluctant to enforce the intellectual property rights of the entertainment industry for a number of reasons. First, and most important to lawyers, are concerns that handing over the details of alleged infringers without a court order could breach the Data Protection Act, be contrary to the obligation to respect personal and private life under the Human Rights Act and may be in breach of the European Directive on Privacy and Electronic Communications. ISPs are also not keen to be charged with 'policing' the internet, as this raises questions as to whether they are suited or qualified to perform what would effectively be a judicial role (i.e. the determination of liability for copyright infringement). ISPs may also argue that they ought not to be

"This has become a politically important and commercially significant issue, engaging policy makers and generating significant press coverage. Whatever the outcome, it is unlikely to please everyone."

“The Department for Business Enterprise and Regulatory Reform (BERR) canvassed views and sought to build a consensus on the best way for ISPs, rights holders and other interested parties to work together to stop illicit P2P file-sharing.”

“According to a government press release, all signatories will strive to engage with and educate users about unlawful file-sharing, make material legally available online in a wide range of user-friendly formats.”

charged with the cost of enforcement, costs which would inevitably be passed on to innocent consumers but benefit only rights holders.

In July, a consultation document was released by the UK Government on the various legislative options open to it to combat illegal file-sharing on the internet. The Department for Business Enterprise and Regulatory Reform (BERR) canvassed views and sought to build a consensus on the best way for ISPs, rights holders and other interested parties to work together to stop illicit P2P file-sharing. In its consultation document, current enforcement procedures were recognised as being inefficient and ill-suited to prevent online piracy. The consultation presented a detailed review of the problem, including the current legal landscape and various alternative means by which the enforcement framework could be improved. BERR's preferred option was a 'co-regulatory approach', striking a balance between the interests of rights holders, ISPs and consumers, and overseen by the independent regulator and competition authority for the UK communications sector, Ofcom.

The Government's consultation paper considers that it is highly unlikely that all ISPs would willingly sign up to a voluntary agreement. Instead it proposes a regulatory solution to create a compulsory framework within which the detailed practical and commercial issues can be resolved, including issues of costs, action to tackle persistent infringement, appeal routes and proportionality. Codes of practice should be agreed between ISPs and bodies representing rights holders it said, and Ofcom should approve any such codes, and provide a regulatory oversight role. Ofcom's involvement should ensure that any self-regulatory mechanism is effective, proportionate and fair to consumers. As part of the consultation BERR also presents alternative options, such as legislation to require ISPs to divulge personal information to rights holders, or legislation to require ISPs to take action against individuals, or to use filtering equipment.

Meanwhile, also in July, a voluntary Memorandum of Understanding, was reportedly signed by the government, the BPI (representing the music industry), the six biggest UK ISPs and the Motion Picture Association. It set out an agreement to work on drawing up codes of practice and to improve consumers' access to legitimate downloads of material. According to a government press release, all signatories will strive to engage with and educate users about unlawful file-sharing, make material legally available online in a wide range of user-friendly formats, and create a self-regulatory environment, with the involvement of Ofcom. The approach will pilot letters to be sent to the registered user of an internet account whose account has been identified as having been used unlawfully to share copyrighted material.

These developments are part of a Government drive aimed at keeping Britain a creative force. Culture, Media and Sport Secretary Andy Burnham said in a press release: "*[the] announcement...holds out hope of a sustainable future for music and our other creative industries, whilst ensuring that consumers continue to get the full benefits that new technology can offer*".

This upbeat message was slightly undermined by reports in the press that Carphone Warehouse, one of the six ISP signatories, had been quoted as distancing itself from any agreement on enforcement strategies and as stating that it had merely agreed to send out letters of notification on behalf of rights holders.

Belgium

In a Belgian decision in 2007, *Sabam v Tiscali (Scarlet)* the Belgian court considered whether an ISP could be required to monitor or filter the activities of their users in order to prevent illicit file-sharing on P2P networks. The court ordered the ISP to install filtering software to prevent its customers from accessing unauthorized music downloads via P2P

networks. The court made this order following expert advice which led it to the conclusion that such a technical solution was possible, practical and cost effective.

The decision was surprising as many, including the ISP involved, had believed that Article 15 of the E-Commerce Directive forbade Member States from imposing any sort of general obligation upon ISPs to monitor the information which they transmit or store. However the court took the view that, while this section related only to the liability of service providers and was meant to prevent ISPs from being found liable for breaching a general monitoring obligation merely because there was illegal material available on its network. The court held that Article 15 was not meant to put a blanket ban on general monitoring obligations. The court referred to clause 40 of the preamble to the Directive: "*the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology.*"

The court ruled that it was entitled to demand that an ISP must monitor internet traffic, and it ordered that the ISP put in place the necessary technical measures to prevent illegal downloading. The judgment is currently under appeal. While the decision of the Belgian courts is not binding on the courts of other jurisdiction, the underlying legal principles of EU law relating to the E-Commerce Directive are harmonised across the EU, and the decision could be persuasive in the UK.

France

In France, the government has made the prevention of P2P downloading into a political issue of great importance. The French government and representatives of the music, film and internet industries entered into an agreement (the Olivennes agreement) in November 2007, under which the government committed to bringing in legislation to prevent infringement of intellectual property rights on digital networks. Also in November, the Creation and Internet Law (CNIL) came into force, creating an independent enforcement authority designed to protect intellectual property on the internet called the "*Haute Autorite pour la diffusion des oeuvres et la protection des droits d'auteur sur Internet*" (HADOPI) and introducing a new criminal offence of having access to a digital network (essentially the internet) and failing to ensure that your connection is not used to infringe intellectual property rights. However, it is a defence for the account owner to show that he has installed one of a list of technologies approved by HADOPI to prevent file-sharing and illegal downloading.

HADOPI operates a 'three-strikes' policy. Where the infringement of IP rights is detected HADOPI can send a customer a warning letter reminding him of his obligations and possible sanctions. If another infringement occurs within six months, HADOPI can send a second warning letter. If another infringement occurs within a one year period of the second warning, HADOPI can suspend the account for between one month and one year, during which time the customer is not allowed to enter into another agreement with another service provider to get internet access. If the ISP does not comply with such a notice, it may have to pay a fine of up to 5000 Euros.

While many, particularly rights holders, will applaud France's robust and decisive approach, others see it as draconian and disproportionate. According to a report by the French government body responsible for overseeing privacy and data protection, the CNIL fails to provide the necessary legal guarantees to ensure an equitable balance between privacy and droit d'auteur (copyright). The CNIL report highlighted a number of privacy issues which were of concern. Among them were that the law gives rights-holders a level of authority normally reserved for the courts and that the law on filtering represented a grave risk to civil liberties, particularly freedom of expression.

"In France, the government has made the prevention of P2P downloading into a political issue of great importance."

This is a hot and contentious issue. According to French news website La Tribune the European Commission has asked the French government to clarify a number of points relating to the internal market and fundamental rights in respect of its CNIL. The Commission's requests have been made public in what appears to be a leaked document. Interestingly, it is reported to want the information before the law is adopted, and therefore appears to be asking France for a halt on the implementation of the CNIL until these questions are answered. The Commission also confirmed that this issue is currently being addressed by the European Parliament and the Council of Ministers in the context of the Telecoms Package review.

The EU's Telecoms Package

Throughout the second half of 2008, the European Parliament has debated and adopted proposals for a new Directive known as the 'Telecoms Package'. The provisional text approved by the Members of the European Parliament in September 2008 included amendment 138, which would have required telecoms regulators to apply the principle: *"that no restriction may be imposed on the fundamental rights and freedoms of end-users without a prior ruling by the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information, save when public security is threatened where the ruling may be subsequent."*

This article lays down the principle that any action restricting use of a network must be in accordance with the requirements of due process and fundamental rights. This amendment is of major importance as it provides protection against non-judicial disconnection and other sanctions against alleged file-sharers. If this amendment were to survive in the final version, which appears unlikely, it would cast severe doubt on the legality of any arrangements where ISPs and right holders seek to disconnect consumers without due legal process.

This version of the amendment was adopted by the European Parliament in an open vote with a large majority of 573 votes in favour and 74 votes against. After the vote President Sarkozy of France wrote to the European Commission requesting that the amendment be removed from the draft legislation. The European Commission refused to do so, responding that it had to respect the democratic decision of the European Parliament. On 7 October 2008 the Commission expressed the view that this amendment was an important restatement of key legal principles inherent in the legal order of the European Union, especially of citizens' fundamental rights. The language of the amendment is deliberately drafted in order to leave Member States scope for reaching a fair balance between several fundamental rights, namely the right to respect for private life, the right of property and effective remedies, and the right of freedom of information and expression. The Commission was therefore happy to accept the amendment proposed by the European Parliament.

However, in another twist in the tale, in November 2008, the European Council (comprising representatives of Member State governments) voted to drop the controversial amendment 138 from the Telecoms Package. In doing so, it set out its position as being at odds with both the Commission and the Parliament. Reports in the French media accused the French government of abusing its role as President of the EU, to have the controversial Amendment 138 removed from the Telecoms Package. This is likely to trigger further debate on whether amendment 138 should be included. It appears that the European Parliament and the Commission will be keen to reinstate it, or something similar, into the Telecoms Package.

"The language of the amendment is deliberately drafted in order to leave Member States scope for reaching a fair balance between several fundamental rights, namely the right to respect for private life, the right of property and effective remedies, and the right of freedom of information and expression."

What next?

2009 promises to be a pivotal year in the development of policies for policing the internet. The results of the UK Government's consultation on legislative options to address illicit P2P file-sharing will be eagerly anticipated. However, any proposals will have to be fashioned in a manner consistent with the outcome of the current tug-of-war between the European Council and the European Parliament relating to this topical and controversial area.



Scott Fairbain
scott.fairbain@cms-cmck.com
+44 (0)20 7367 2134



Anne-Laure Villedieu
anne-laure.villedieu@cms-bfl.com
+33 1 47 384019

Technology, Media and Telecoms – Expertise

CMS Cameron McKenna LLP 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 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.

This bulletin is intended for clients and professional contacts of CMS Cameron McKenna LLP. It is not an exhaustive review of developments in the law and is intended to simplify and summarise the issues to which it refers. It must not be relied upon as giving definitive advice.

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

CMS Cameron McKenna LLP is a limited liability partnership registered in England and Wales. It is able to provide international legal services to clients utilising, where appropriate, the services of its associated international offices and/or member firms of the CMS alliance.

The associated international offices of CMS Cameron McKenna LLP are separate and distinct from it.

CMS Cameron McKenna LLP and its associated offices are members of CMS, the alliance of independent European law firms. Alliance firms are legal entities which are separate and distinct from CMS Cameron McKenna LLP and its associated international offices.

CMS offices and associated offices worldwide: Amsterdam, Berlin, Brussels, London, Madrid, Paris, Rome, Vienna, Zurich, Aberdeen, Algiers, Antwerp, Arnhem, Beijing, Belgrade, Bratislava, Bristol, Bucharest, Budapest, Buenos Aires, Casablanca, Cologne, Dresden, Dusseldorf, Edinburgh, Frankfurt, Hamburg, Kyiv, Leipzig, Ljubljana, Lyon, Marbella, Milan, Montevideo, Moscow, Munich, New York, Prague, Sao Paulo, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Utrecht, Warsaw and Zagreb.

www.cmslegal.com

The members of CMS are in association with The Levant Lawyers with offices in Beirut, Abu Dhabi, Dubai and Kuwait.