C/M/S/ Cameron McKenna

Technology Annual review

A month by month review of selected technology legal news from 2005

March 2006

Foreword

Phillip Carnell

Welcome to the very first CMS Cameron McKenna technology annual review. The review looks at the year that was 2005 and for each month provides an interesting mix of articles based on events which took place in that month.

I hope you will find something of interest in each month's articles. However, my favourite month is February, where there are articles on: the legality of Denial of Service attacks; Microsoft's success in using criminal law evidence in a software copyright infringement claim; the courts attempt to put a hold on the number of "Internet defamation" cases brought in the UK; Alistair Campbell's free advertising for Blackberry (by accidentally launching a foul-mouthed tirade against the BBC); and Europe being crowned "Internet Villain" at the ISPA awards.

This isn't something we have ever done before so please be gentle with us and, more importantly, let us know what you think about the publication. We intend to publish an Annual Review every January from 2007 onwards (just a little bit earlier than this year!), so please let us know about what you like and dislike about this year's copy. If there is anything you would like to see or would find useful in next year's publication, please let us know about that too.

To collate opinions, we have set up an online survey which can be accessed at **www.law-now.com/TAR2005.** You can also link to a digital copy of this document at the same address.

Happy reading, and wishing you good luck in what remains of 2006.

Phillip Carnell
phillip.carnell@cms-cmck.com

January

February

March

April

May

June

July

August

September

October

November

December

Everyone's talking about *Navitaire v easyJet*...

At the beginning of 2005, technology and IP lawyers everywhere were still talking about the judgment in *Navitaire v easyJet and BulletProof* which was finally published in December 2004. The case provided an interesting and important insight into how the English Courts are likely to apply the laws of copyright to computer software and its development.

The case concerned the claimant's (Navitaire's) software, which was designed to operate a ticketless airline booking system. The first defendant, easyJet, previously licensed and used the claimant's software. The second defendant, BulletProof, was employed by easyJet to produce new software to replace the claimant's software. Together, the defendants set out to replicate the claimant's software program so that the new software produced was "substantially indistinguishable" from, and had the same "look and feel" as, the claimant's software. Despite these blatant acts of copying, because copying of the software's source code itself was not involved, the defendants were in most respects held not to have infringed the claimant's copyright in the software.

The defendant's software used identical input codes (which produced identical outputs) to the claimant's software. Some codes were complex, for example A[departure date][city pair]/[return date](optional +[days].[fare class]), and the defendants had also copied these. However, the Judge held that no copyright subsisted in any of the codes (or all of the codes together as a compilation) for two reasons. First, the codes were not recorded in the source code (or anywhere else in the software) as the software was designed to 'parse' the complex codes "bit by bit" rather than as a complete code. The codes were not therefore "recorded" which is required for literary copyright. Secondly, the Judge held that the codes were a "computer language" which cannot be protected by copyright.

One of the most interesting claims made by the claimants was that there had been a "non-textual" copying of the software, and that the "business logic" behind the software had been copied. The claimant based its legal argument on an analogy between the function of the computer program and the plot of a literary work, which had been successfully argued in previous cases. Here, however, the Judge decided that the analogy was a poor one and that the relevant "skill and labour" had not gone into creating the "business logic" of the software. As a result, the "business logic" of the program could not attract copyright protection.

The judgment confirms the position that the law of copyright will protect computer software, but only if the source code of such software is substantially copied. There may remain some scope to argue that the architecture or structure, or even the business logic, of computer software has been substantially copied. However, for copyright to subsist in those elements of the computer software, a relevant amount of the author's skill labour and judgement must have gone into designing them.

On the face of it, the court's decision appears unjust. Navitaire's licensee set out to copy its software package but, because of the way it was copied, Navitaire was not successful in claiming protection (or recompense) from the law of copyright. For much of 2005, there was talk (and much excitement) about whether Navitaire would appeal the decision, having obtained permission to do so. However, to the disappointment of many, it was confirmed in November 2005 that the parties had reached an out of court settlement and that there would be no appeal.

New standard Government IT contracts published

In 2004 the Government announced that it planned to move away from PFI as a method of financing government IT projects. After months of consultation with the IT industry, the Office of Government Commerce (OGC) finally published two new sets of standard contract terms for use in the tendering process for public sector IT contracts.

One contract, the Model Technology Supply Agreement (MTSA), covers the supply of IT goods. The other contract, the Model IT Services Agreement (MISA), relates to procurement of IT services. The agreements contain extensive guidance notes and a number of optional clauses which may be deleted depending on the nature of the particular project.

Both new agreements need to be read in conjunction with the OGC's "commercial principles" contained in its "decision map" guidance, which is available on the OGC website. The guidance makes salutary reading for anyone negotiating, or otherwise dealing, with government bodies (which will be using the same guidance).

The OGC hopes that use of the new contracts will simplify the tendering process and result in time and money savings for both IT suppliers and public sector bodies.

BAA loses fight for gatwick.com

BAA plc took action against the owner of the domain name **gatwick.com** claiming that it was confusingly similar to BAA's registered trade marks, and that it otherwise infringed BAA's unregistered rights in the use of the name "Gatwick". The action was brought at the Arbitration and Mediation Centre of WIPO under the Uniform Domain Name Dispute Resolution Policy (UDRP).

The domain name **gatwick.com** was being used by its owner to offer directory services to local businesses which operated services near Gatwick Airport, for example local hotels. The website did not attempt to show an association with BAA or its airport business.

BAA plc lost its claim, and was not therefore entitled to the domain name gatwick.com, despite having trade mark registrations for "BAA Gatwick" and unregistered rights in the name "Gatwick" connected with the airport. The respondent was found to have been using the domain name "in connection with a bona fide offering of goods or services" (UDRP 4(c)(i)) and therefore had existing legitimate rights or interests before the complaint was made by BAA plc.

January

A good month for…

Anyone against the introduction of Software Patents

MEPs from 13 different countries called for the draft Directive on the patentability of computer implemented inventions to be scrapped and resubmitted to the European Parliament for approval. The motion started a roller coaster of a year looking at the issue of software patents and whether or not they should be formally recognised in EC law.

A bad month for…

Retailers offering extended warranties

The Government published the text of the Supply of Extended Warranties on Domestic Electrical Goods Order 2005 in January 2005. The new legislation was introduced to deal with concerns about the mis-selling of extended warranties on electrical goods. It includes (much to some retailers' dismay) a non-excludable 45 day cancellation period.

January

February

Denial of Service Attacks, are they illegal or not?

March

April

May

June

July

August

September

October

November

December

The issue of criminal liability for Denial of Service (DoS) attacks separately made the news twice in February 2005. First, the All Party Internet Group called for a Bill to be introduced into Parliament specifically to add a DoS offence to the Computer Misuse Act. Secondly, almost conversely, criminal charges were brought against a person for offences under the Computer Misuse Act in respect of a DoS attack.

A DoS attack is an attack against a computer system which overloads the system with data or information requests causing it to crash, or which significantly degrades the service provided by the system. DoS attacks rarely present a security threat, but they can cause huge inconvenience and can cost the target company a large amount in IT costs and/or lost revenues.

It is unclear whether the current wording of the CMA covers DoS attacks. The wording of Section 3(1) of the CMA states that it is an offence to cause an "*unauthorised modification of the contents of any computer*". There are valid arguments to suggest that unauthorised modifications are made to a computer when it is subject to a DoS attack, but there are also equally valid arguments that the opposite is true. It is generally agreed that the wording probably covers some DoS attacks, but this is only because third party computers are used without permission to launch the DoS attack; the DoS attack itself may not be an offence.

Unfortunately, APIG's proposed bill was given just 10 minutes of Parliament's time and taken no further. However, the Police and Justice Bill, due to be published in early 2006 is likely to include amendments to the CMA which take account of the APIG's recommendations.

Also in February 2005 the press reported that charges had been brought against a man in Scotland in relation to a number of DoS attacks, allegedly made against the owners of a number of online operations both in Scotland and the USA. The man was released on bail pending further inquiries by the police.

It was only the second time that charges have been brought under the CMA for the launch of a DoS attack. In 2003, similar charges were brought against a teenager from Dorset who was accused of launching a DoS attack. In that case the jury acquitted the accused because he successfully argued that a third party with access to his computer had carried out the attack, via the use of a trojan virus. The case did not therefore address whether the offences under the CMA could apply to a DoS attack.

Until the issue is decided at trial, it will remain unclear as to whether the CMA could apply to DoS attacks. Clarification by Parliament is much needed and would be welcomed by industry. It is hoped that the 2006 Police and Justice Bill will provide such clarification.

Using criminal law evidence in civil proceedings

In 2002, two individuals were convicted in the criminal courts for conspiring to defraud Microsoft by dishonestly dealing in counterfeit Microsoft software. Microsoft subsequently took civil action against the two individuals and, in applying for summary judgment, attempted to use evidence of the criminal convictions to show that the defendants were liable in civil law.

At the summary judgment hearing, the Judge held that evidence of the criminal convictions could be used and was sufficient to establish the civil liability of the defendants. In the circumstances, there was no real prospect of the defendants successfully defending Microsoft's claim that they were liable for infringing Microsoft's copyright and trade marks, and for passing off.

However, Microsoft was not successful in obtaining an interim payment order against the defendants. None of the criminal evidence went to the amount of any profits the defendants had made in selling counterfeit products. In particular, Microsoft were unable to prove, and the criminal evidence did not show, the proportion of products sold by the defendants which were counterfeit.

Small Internet defamation cases an "abuse of process"

English defamation law is seen to be relatively "claimant friendly" and, as a result, it is common for claimants to bring defamation proceedings in England in respect of publications on the Internet. Previous cases have shown that proceedings may be brought in England if: (a) the defendant has a reputation in England; and (b) the publication was able to be read or downloaded in England (i.e. even if the publication was not aimed at English readers).

In the case of *Jameel v Dow Jones*, the claimant, who was based in the UK, objected to allegations made about him on the US Wall Street Journal website and issued proceedings in the English courts. The evidence showed that the allegedly defamatory material had only been downloaded five times in the UK.

The Court of Appeal held that a real and substantive tort had not occurred in the UK. As such, to commit substantial resources of the court to an action where so little was at stake was an abuse of process. The case shows that there are limits to the jurisdiction the English courts are prepared to accept, in particular where limited damage has been suffered in the jurisdiction.

February

A good month for…

RIM/Blackberry

Alistair Campbell gave RIM, the manufacturers of the Blackberry device, some free advertising. He also gave everyone else a lesson in why you should be careful with email, particularly email on the move. Mr Campbell used his Blackberry to email a BBC Newsnight journalist suggesting that the BBC should "f**k off and cover something important" and referred to BBC journalists as "T**ts". He later claimed that he had sent the email by mistake, intending it to go to an advertising agency.

A bad month for…

'Europe'

Europe was crowned Internet Villain for 2005 at the annual ISPA awards. It received the award for threatening to remove the "country of origin" principle, which has encouraged e-commerce across the EU, and for its proposed directive on data retention (now passed and giving ISPs a headache in 2006). Needless to say, a representative for the EU did not turn up to collect the award.

January

February

March

April

May

June

July

August

September

October

November

December

The Court of Appeal speaks...

The judgment in *Peregrine Systems v Steria* (14 March 2005) provided a rare opportunity to see how the Court of Appeal would deal with a dispute about the terms of an IT contract. The facts of the case are complex, but the principle behind the judgment is simple: do not enter into a "services" contract with an IT service provider if you need an implementation project completed for a specific sum or within a specific timeframe.

The contract provided Steria with a non-exclusive licence to use Peregrine's call centre software packages, and required Peregrine to provide services to install such software on Steria's hardware. Steria terminated the contract because Peregrine did not complete implementation on time. Peregrine argued that it had provided £200,000 worth of services, which is all it had contracted to provide, and that Steria had wrongfully terminated the contract. Steria counterclaimed that, as a result of repudiatory breaches of contract and/or misrepresentations by Peregrine, it was entitled to terminate the contract.

The Court of Appeal confirmed the High Court's decision that, on the terms of the contract, Peregrine had not contracted to complete implementation, but only to provide £200,000 worth of services. Services to that value had been provided. After that date, therefore, Steria was free to obtain services from whoever it chose to complete the implementation. This was because there was no express provision as to what had to be completed for that sum of money and by what time.

When looking at the wording of the contract, the Court of Appeal took a commercial approach to interpretation, considering specific clauses in the context of the whole arrangement. The Court of Appeal also expressed the view that Steria had acted in a way which suggested an election to affirm the contract (after Peregrine had committed an anticipatory breach of contract), for example, Steria's continued use of the software, technical support services and training.

This case highlights the importance of ensuring that IT software contracts expressly state that an implementation project is to be completed for a specified sum. Steria had attempted to do so by placing a £200,000 limit into the schedule which described the work, however this wasn't sufficient to show an obligation to **complete** the project for a sum, since the schedule itself showed the obligation to prepare a "blueprint" suggesting that at the time of contract the parties did not know how long it would take or what the costs would be.

Although services are often provided on a time and materials basis, because the timings are not easily predictable, where possible, the cost of a software implementation project should be ascertained at the outset and, if certainty is required, the supplier of the software made to commit to completing the project for that sum, or at least to within a reasonable margin. This will help to manage expectations and minimise disputes.

Anonymous poster settles

In 2003, a fund manager posted a number of false allegations on the discussion board on the Motley Fool website. The allegations made were about the Chief Executive of a large financial services group. The allegations were viewed 49 times online before they were taken down by the website administrators.

Motley Fool was ordered to reveal all details that it had on the anonymous poster, including his or her IP address. The IP address led to the anonymous poster's employers who revealed his identity. Once the poster's identity was revealed, proceedings were commenced against him. In March 2005, the proceedings were settled - the anonymous poster agreeing to make a public apology and pay damages and substantial costs to the claimant.

The case illustrates how the courts will order ISPs and website operators to reveal the identity of anonymous wrongdoers using pseudonyms. Although this case did not end with a court decision, the publicity surrounding the case resulted in many ISPs and website operators issuing new codes of conduct and terms and conditions to its users. The underlying message being that very little, if anything, can be done on the Internet which is truly anonymous.

Apple grabs 'itunes.co.uk'

In October 2000, Apple obtained the trade mark ITUNES. However, it did not start operating its iTunes service using the domain *itunes.com* until June 2004, when it quickly built up a huge international reputation. The respondent, a company called Cyberbritain, registered the domain name *itunes.co.uk* in November 2005. This was after Apple's trade mark registration but before Apple began operating the iTunes service.

Originally Cyberbritain had used the *itunes.co.uk* domain name to direct users to its legitimate music download site. However, it then used it to direct users to its gambling website and, in October 2004, it directed users to the Napster website, a direct competitor of iTunes. Apple offered to purchase the domain name for $5,000 US Dollars. Cyberbritain offered to sell it for £50,000. At this stage, Apple commenced the Nominet dispute resolution procedure.

The Nominet expert found that the offer to sell the domain name for £50,000 did not, by itself, take unfair advantage of Apple's rights. The offer was made in response to an approach from Apple to purchase the domain name. However, the expert found that Cyberbritain had taken unfair advantage of Apple's rights by offering to sell the domain name to Napster and by redirecting users to Napster's website. Such action allowed a competitor of Apple to benefit from the goodwill that Apple had built up in the iTunes' name. Apple was therefore awarded the transfer of the domain name itunes.co.uk.

March

A good month for…

The BPI

The British Phonographic Industry (BPI) announced that 23 UK Internet users had agreed to pay thousands of pounds in compensation for distributing music illegally via peer-to-peer networks on the Internet. To keep the pressure on those still engaging in illegal file sharing, on the same day the BPI announced that it was going to apply to the courts to force ISPs to reveal the details of another 31 file sharers from across the UK (see page 12).

A bad month for…

Global Internet Harmony

The famous Yahoo! case about Nazi memorabilia auctions reared its ugly head again when Yahoo! approached the US Courts for an order that its Yahoo.com site is not bound by an earlier decision of the French Courts that all Yahoo! sites accessible from France must not operate Nazi memorabilia auctions. Yahoo.fr had complied with the order of the French court, but Yahoo! claimed that Yahoo.com should not be bound by the order, despite it being available to French users.

January

February

March

April

May

June

July

August

September

October

November

December

New Fraud Bill covering technology offences published

In April the Government published the new Fraud Bill. The Bill's aim is to make phishing attacks and online credit card fraud a thing of the past by updating the law relating to fraud in light of technological advancement. Under the existing law of fraud, criminals were able to escape liability easily by arguing that their crimes did not fit within the outdated narrow definitions in the existing legislation. Under the Bill, Internet fraudsters and phishers could be subject to ten year prison sentences.

The new Bill creates a general offence of fraud which can be committed by false representation, failing to disclose information and abuse of position. New offences for obtaining services dishonestly and possessing, making and supplying articles for use in fraud have also been created. The Bill has been specifically drafted to catch illegal activities which involve the use of technology.

"Phishing" will be caught by the offence of fraud by false representation. A "phisher" sends an email to his victim which falsely represents that the email has been sent by a bank or credit card company, prompting the reader to confirm/provide personal information such as account numbers. The phisher then uses that information to "phish" any money out of the account. The offence will also apply to a person who dishonestly uses a stolen credit card online to pay for items. That person, by his conduct, is making a false representation that he has the authority to use the card and is committing an act of fraud, regardless of whether an online retailer is deceived by the representation.

The Bill includes the crime of "fraud by abuse of position". The term "abuse" is not defined and the explanatory notes make it clear that it is intended to cover a wide range of conduct. This may have a number of applications in relation to technology related crime. For example, it could apply to an employee of a software company who uses his position to copy software products with the intention of selling the copied products as original copies.

The definition of "Article" in the crime of "possession, making and supplying articles for use in fraud" has been defined widely. The definition includes programs/data held in electronic form, covering those in possession (or the makers or suppliers) of computer programs used to generate credit card numbers or produce blank utility bills, and computer files that store data for fraudulent use.

Finally, the Bill has created an offence of "obtaining services dishonestly". This offence replaces and is wider than the current offence of obtaining services by deception and, as a result, "deception" is no longer required. The scope of the offence will now include activities such as obtaining services over the Internet using false credit card details and using a decoder to obtain satellite TV channels without paying.

With identity theft and credit card scams becoming a growing concern, the new legislation is welcomed and, in theory, should result in a considerable increase in prosecutions for technology related crimes.

"Drink or Die" hackers given prison sentences

Four members of the infamous 1990s "warez" software piracy group "Drink or Die" were jailed for conspiracy to defraud. Drink or Die was formed in 1993 and at its peak had around 60 members. Two members that pleaded guilty to cracking software and recruiting new group members were sentenced to 18 months each. The two other members, who had pleaded not guilty, received 24 and 30 months for their roles as software suppliers to the group.

Drink or Die is most famous for releasing a fully functioning version of Windows 95 two weeks before Microsoft. The group did not aim to financially gain from its software piracy, indeed it was frowned upon by the group, but were instead motivated by the cachet of being the first to break the code of new software. The problem for the owners of the software cracked by the group was that the cracked software often ended up in the hands of organised criminals, who were then able to mass-produce and sell the pirated software. The owners of the software were therefore keen to track down and prosecute those responsible for cracking the software.

As a result of the US customs-led investigations into Internet software piracy in 2000, more than 70 properties were raided at the same time in Australia, Finland, Norway, Sweden, the UK and the US. More than 60 people were arrested including eight in the UK. Of those eight people, four were the defendants sentenced for conspiracy to defraud.

UK bans online porn sales

In the UK, certain pornographic material (e.g. R18 dvds) may only be sold in licensed premises where there is a face-to-face meeting between buyer and seller. Trading Standards regularly take action against UK companies which sell restricted material over the Internet or by mail order.

Two sex shop owners took action against Trading Standards to appeal a fine they had been given by Liverpool magistrates court for selling restricted material by post. They argued that there was "no sensible purpose" in preventing adults obtaining restricted material videos by mail order from within the UK when Customs allowed similar videos to be imported by mail order.

The judgment from Lord Justice Kay and Mr Justice Newman held that the existing rules were in place to attempt to prevent sales to underage customers. The reason for ensuring a face-to-face meeting between buyer and seller was to make sure the buyer was old enough. It was accepted that such restrictions could be subverted, but that did not justify removing them.

The Court rejected all arguments raised by the sex shop owners and the appeal was not allowed. The Judges recognised, however, that the matter was one of national importance, and they therefore granted permission for an appeal direct to the House of Lords.

April

A good month for…

The Waterstone's Blogger

A Waterstone's employee who was sacked for referring to his boss as "Evil Boss" and to his employers as "Bastardstone's" in his blog, won his appeal against his dismissal. However, an offer of reinstatement at Waterstone's was rejected by the blogger and, according to press reports, the parties reached an "amicable settlement".

A bad month for…

Fingerprint recognition

Malaysian thieves attempted to steal an S-class Mercedes. Unfortunately for the owner of the car, when the innovative thieves realised they could not start the engine because the car would not recognise their fingerprints, they decided to obtain a finger which the car would recognise. The owner was kidnapped and woke up at the side of the road…with one finger missing.

January

February

March

April

May

June

July

August

September

October

November

December

The BPI obtains the names and details of another 33 people it suspects of sharing music files

In October 2004 the British Phonographic Industry (BPI) announced that it had commenced a rolling programme of legal action against "major file sharers". In May 2005, round two of such action began as the BPI made a further application to the high court for an Order requiring various ISPs to hand over the personal details of another 31 alleged peer to peer (P2P) file sharers.

The BPI has made it clear that they are only pursuing those file sharers who are "large-scale uploaders". This reflects the fact that proving loss against someone who only downloads music, above the amount of profit the recording company would have made if the P2P downloader had legitimately downloaded the recording in question, would be very difficult, and the amount of damages obtained would be small.

If the BPI is able to prove, on the balance of probabilities, that a person has uploaded a number of tracks to other P2P users, then although proving loss will still be very difficult, the amount of damages could be significantly higher.

A problem for the BPI is that, if they are successful in obtaining a judgment against an individual, the damages may be too small to act as a deterrent to other uploaders. The BPI states that its main objective in taking legal action is to discourage illegal uploading. However, the complexity of obtaining significant damages against a P2P uploader may result in a small amount of damages being awarded and which, therefore, may even have the opposite effect. It is for this reason that the BPI may decide in favour of making well-publicised financial settlements with the file sharers so that the threat of legal action remains a deterrent to other P2P users.

The BPI, and other such organisations worldwide, clearly have a difficult job to do to raise awareness about the problems of file sharing and to try and prevent people illegally downloading tracks. A particular challenge for the BPI will come from the fact that P2P has evolved and, even if the BPI is successful in discouraging one form of P2P file sharing, it is likely that another form of file sharing will become more popular.

The most likely solution for the BPI, and other such organisations worldwide, will be to ensure that legal downloading sites offer a service which is a real alternative to using P2P software. This means that such services will need to compete on price and, often something that makes illegal downloading attractive, on release dates. The good news for the BPI is that, combined with the threat of legal action (and the unknown consequences of such action), the increasing popularity of existing online music services, such as Apple's iTunes, may have already had an impact on the number of people using P2P.

WIPO orders the transfer of tmobil.com to the owners of T-Mobile

Deutsche Telekom, the owners of T-Mobile, brought a UDRP complaint at the Arbitration and Mediation Centre of WIPO against the owners of the domain name *tmobil.com*. The domain name had passed through the hands of several owners (as they attempted to avoid legal action by Deutsche Telekom) before ending up in the hands of Mighty LLC, the respondent to the UDRP action.

Mighty used the domain name for a website which was headed "sponsored links" and advertised and provided links to mobile phone retailers. At the bottom of the page were the words "Copyright 2005 tmobil.com". Deutsch Telekom claimed to have rights in the name t-mobil, and argued that Mighty had no legitimate interest in the domain name, and was using it in bad faith.

The WIPO panel decided that the domain name was being used in bad faith and that Mighty had no legitimate interest in it. Factors commented on by the panel were that Mighty did not offer any goods or services itself using the domain name, that Mighty did not exclusively offer T-Mobile products and services (i.e. it was not using the domain name to legitimately identify services it provided), and that the website did not make it clear that there was no affiliation between the two parties. The panel directed that the domain name should be transferred to Deutsche Telekom.

PC World found guilty of "mis-selling"

A Yorkshire court found PC World guilty under the Trade Descriptions Act 1968 of mis-selling computer equipment. Trading Standards had brought the prosecution because buyers of "new" computer equipment from a Yorkshire branch of PC World had discovered that the equipment was, in fact, second hand. The two examples given in the press were of a laptop and an Apple CDRW, both of which were sold as "new", but were actually reconditioned or returns.

Despite protestations from PC World that the mis-selling had occurred as a result of "honest mistakes" caused by its computer system and individual errors, the court fined the company £5,500, awarded its wronged customers over £2000 each in compensation, and ordered the company to pay £28,000 in prosecution costs. The Judge also attacked PC World's staff training, which was insufficient to prevent such mistakes happening.

The case shows that retail businesses must be careful when describing goods for sale, in particular where goods are ex-display, reconditioned goods, or returns. Any description of goods given must be accurate and not misleading. It also shows that, if criminal proceedings are brought by Trading Standards, the prosecution costs could far outweigh any fine ordered by the court. In this case the costs were 500% more than the fine.

May

A good month for…

American iPod owners

Apple was forced to settle a number of US class actions brought in relation to the battery life of the iPod. It offered extended warranties and $50 store credits to consumers who had filed complaints. Apple had claimed a battery life that would power uninterrupted play for ten hours. However, many had found that the batteries held their charge for only four or five hours. This had prompted the class action.

A bad month for…

The DTI

A number of articles were published which showed that the DTI's 2004 consultation into spam was flawed. The DTI asked in the consultation if spam to businesses should continue to be allowed or whether anti-spam legislation should be should be introduced to prevent it. An information request under the Freedom of Information Act, showed that the DTI received, and accepted, a huge number of responses from direct marketing companies – who may have been responsible for the spam in the first place.

January

February

March

April

May

June

July

August

September

October

November

December

E-Data patent for the downloading of data from the Internet found to be invalid

E-Data owned a patent which concerned a system for reproducing information in "material objects at a point-of-sale location". The method and apparatus claimed enabled articles (such as CDs) embodying information (such as sound recordings) to be manufactured on demand at the place where they are sold under the control of the "owner" of the information – i.e. the copyright holder or his licensee.

E-Data tried to use its patent to take action against Getty Images. Getty Images supplied digital copies of images from libraries accessible over the Internet via their websites. Customers who wished to reproduce these images entered into a licence agreement whereupon they could download digital copies of the images on to their computers and thereafter reproduce them as required. In response, Getty Images claimed that E-Data's patent was invalid because it lacked novelty.

As is so often the case with patent infringement claims, the court's construction of the various claims for the patent was central to the case. E-Data claimed that the invention embraced a system in which additional copies of legally downloaded information could be made. The Defendants, on the other hand, said that such a system was outside the scope of the invention and that the invention could not be used to make further copies, unless a further request was made from the owner of the information. The Defendant's interpretation was preferred, not least since it provided "a coherent explanation for the function and inter-relationship of the various features of the claims".

Further significant issues concerned the construction of the named term "point of sale location". The defendant submitted that it could only be a location where "material objects" embodying information were sold and purchased. The patentee contended that a "point of sale location" could be any location where a consumer can purchase a material object or where there are means to make such a material object himself – for example using a CD re-write function on a home computer. Once again, the defendant's construction was preferred. It was held that, if this was what the inventor intended, it would have been easy for him to draft the patent that way and unnecessary for him to include a definition of "point of sale location".

For the above reasons, the patent was found to be not infringed. Further, in light of the construction given, the patent was in any event found to be invalid as lacking novelty and obvious over cited prior art.

The case will be of interest to both patent lawyers and the IT community. It represents a further example of a case where a patent directed to the sale of physical products was unable to be enforced in respect of activities carried out over the Internet.

Record Companies' Victory in Peer-to-Peer Case

To much excitement, the US Supreme Court gave its judgment in *MGM v Grokster* at the end of June. The judgment reversed the decision of the 9th Circuit Court and held that Grokster (the creator of the peer-to-peer software sharing program) was liable for contributory copyright infringement.

The 9th Circuit Court had held that, because there were significant non-infringing uses of the peer-to-peer software, there was no copyright infringement by Grokster. However, the US Supreme Court held that the existence of significant non-infringing uses is not sufficient to avoid liability if there is a clear intent to induce copyright infringement.

The plaintiffs' case was assisted greatly by documents disclosed by the defendants, which revealed an intention on the part of Grokster to induce infringement in order to make more money. Such evidence persuaded the court that Grokster was in the business of promoting and inducing illegal file transfers. They were therefore liable for contributory infringement.

The case was a big victory for the record companies, who will no doubt proceed to use the decision to take action against any other party creating or distributing peer-to-peer software in the US. However, the decision does make it clear that having the relevant intent is crucial for a finding of contributory liability. Future peer-to-peer software creators will therefore be able to use the decision to modify their activities to ensure they are protected from similar action being brought against them.

Nominet's Appeal Panel split

Nominet's DRS proceedings commence with a decision from a single expert. If that decision is appealed, the appeal is heard by three experts sitting together. The identity of the expert and their approach in applying the DRS policy will affect the outcome of a domain name decision.

In 1994, vikingdirect.co.uk was registered by a director of a company which was in dispute with Viking Office Products, Inc, which owned the trade mark VIKING DIRECT. Viking invoked Nominet DRS proceedings after making several attempts to purchase the domain name. The original Nominet expert found that, although Viking had the requisite rights in the "Viking Direct" name, it had failed to demonstrate that the domain name was an abusive registration.

Viking appealed and argued that the registration of a domain name by a customer of a business, which contains the established trading name or registered trade mark of that business, should give rise to a presumption that such registration is abusive. The three expert appeal decided by a majority vote not to allow the appeal.

The dissenting expert was of the view that the registration of a well known (or known to the person making the application) name as a domain name called for an explanation, and that failure to provide such explanation should lead to a finding of abusive registration. Had the dissenting expert been the original expert, it is likely that the first decision would have been different.

June

A good month for…

Anyone who dislikes NTL

A disgruntled NTL customer was found not guilty of sending a grossly offensive message, after he had accidentally found a way to change NTL's recorded message - played to those waiting to speak to customer services. Wonderfully, he changed the message to: "*You're through to NTL customer services. We don't give a f**k about you. We're never here. Just f**k off and leave us alone*"

A bad month for…

Indymedia

Indymedia offers users of its website the ability to make anonymous postings. To do so, it claims not to log IP addresses of those posting messages on its forum. This month, the police seized Indymedia's server after it refused to reveal the identity of an anonymous bulletin board poster who had posted a message about an attack on a freight train.

January

February

March

April

May

June

July

August

September

October

November

December

Software copyright licences are just different, ok!

On 14 July the court gave its decision in *Clearsprings Management v Business Link*. Clearsprings had commissioned Business Link to develop software for a web-based database. Business Link used generic code, which it had created for a previous internal project, to commence development of the Clearsprings software.

The contract did not contain an express term dealing with ownership of the copyright in the software. In particular, it did not contain an assignment of the legal ownership of the copyright to Clearsprings. As such, in the absence of express written agreement to the contrary, legal ownership of the copyright went to the contractor, Business Link.

Clearsprings brought an action against Business Link claiming that despite a lack of express terms in the contract, there was an implied term that all copyright in the commissioned software would be assigned to them, or alternatively that they should be granted an exclusive licence to repair, maintain and upgrade the software and sub-licence it to third parties on the grounds that:

- the software constituted Clearsprings' specific procedures in electronic form;
- Business Link had worked closely with Clearsprings' employees to jointly develop a work based on substantial amounts of information supplied by Clearsprings;
- the contract price was consistent with such implied terms; and
- the implied terms would have a limited impact on Business Link.

The Judge held that in the circumstances it was not necessary to imply a term into the contract giving Clearsprings an assignment or an exclusive licence. Instead, the only implied term necessary to give the contract business efficacy was a non-exclusive, perpetual, irrevocable, royalty-free licence for Clearsprings to use the software for the purposes of its business under which it was entitled to repair, upgrade and maintain the software in accordance with the needs of its business but not to sub-licence. The Judge commented that Business Link would in any event be restricted from making use of the information about Clearsprings' operating procedures by the law of confidence.

This case shows the problems that may be incurred if it is not clearly established who owns the copyright in software developed for a client by a contractor. As a copyright work, software causes particular problems because, in developing a system for a client, a developer will often reuse existing work. For this reason, it is unusual for software developers to hand over complete ownership of the copyright to the commissioning party.

The case highlights the difference between how the courts will deal with software as a copyright work as against other copyright works. It demonstrates that the courts will take into account established trade practices and specific types of work in order to consider the implied terms required to give an agreement business efficacy.

Patent Applications GB 0226884.3 and 0419317.3 by CFPH

According to section 1(2) of the Patents Act 1977, business methods and computer programs "as such" are excluded from patentability. However, a series of cases in the UK over recent years and the practice of the UK Patent Office (UKPO) shows that software which provides a technological effect, and has the capability of being applied in industry, will be treated as patentable subject matter.

This approach was reconfirmed by the Patents Court in the matter of Patent Applications GB 0226884.3 and 0419317.3 by CFPH LLC (CFPH). The two patent applications in issue related to computer-networked interactive wagering on the outcomes of events. The patent applications were rejected by the UKPO because they were "business methods" and did not provide a technical contribution.

On appeal, the court agreed with the UKPO decision and set out a new 2-stage test (subsequently endorsed and applied by the UKPO). The new, 2-step procedure is to: (i) identify what is the advance in the state of the art that is said to be new and non-obvious (and susceptible to industrial application); and (ii) determine whether it is both new and non-obvious (and susceptible to industrial application) under the description of an "invention".

Despite the new test, the UK position in relation to the patentability of software (and certain other excluded subject matter) remains in some respects unclear. What is clear, however, is that provided that part of an invention is new and has a technical effect, it may be patentable even if it is software.

Grey Imports – why bother?

In 2005 a large number of trade mark owners were successful in taking action against importers of grey market goods (i.e. goods first placed on the market outside of the EEA). The July 2005 case of *HP and Compaq v Expansys* is a good example of the ease in which trade mark owners are able to obtain summary judgment against the importers of such goods.

Expansys sold numerous HP products which it sourced from Asian distributors. In particular, Expansys sold large quantities of HP iPAQ PDAs previously manufactured and sold by Compaq. HP and Compaq took action against Expansys for trade mark infringement (for importing the Asian sourced iPAQs without permission) and applied for summary judgment.

Expansys argued that it had the following, at least arguable, defences: (i) that HP had delayed in taking action for two years; (ii) that HP had full knowledge of the oversupply to the Asian market and to the grey import practice; and (iii) that the claimants' anti-competitive behaviour meant they were not entitled to prevent such importation. The court took the view that none of the defences claimed had any real prospect of success and HP were therefore awarded summary judgment.

July

A good month for…

Anyone who can't stand the Crazy Frog

Ofcom announced that it would be investigating the company behind the Crazy Frog (you know, "*ring, ding, ding, mnarr, ring, ding ding*" etc etc ad infinitum) for signing up people to premium rate subscription services without consent when the ringtone was downloaded. Three cheers for Ofcom!

A bad month for…

J K Rowling

OK, OK, actually a very good month because of the number of sales of Harry Potter and the Half Blood Prince. But JK Rowling was also the victim of the efficiency of modern day pirates as, within days of its release, the book had been scanned in, OCR'ed, and offered for download as a text file.

January

February

March

April

May

June

July

August

September

October

November

December

Is source code an insured loss? Probably, maybe...

Tektrol designed, developed and manufactured energy saving control devices for industrial motors. Its most successful product contained software which could be easily customised to the needs of a particular customer. To protect the source code, Tektrol stored it in five different places: on two development computers at its premises, on a laptop belonging to the Managing Director, on a computer at a remote site operated by an independent company and on a paper printout kept at the premises.

In a bizarre chain of unfortunate events, all copies of the source code were lost or destroyed. First, the Managing Director received an email containing a virus, which destroyed the copy of the source code on the laptop and at the remote site. Then Tektrol's premises were burgled and the development computers containing the source code and the paper copy of the code were stolen.

Tektrol brought an action seeking an indemnity from its insurers for contents, stock and business interruption losses caused by the loss of the source code due to the virus and the burglary. The insurers claimed that the losses were excluded under the policy. By clause 7(b)(i) of the policy, damage or consequential loss caused by the erasure, loss, distortion or corruption of information on computer systems or other records, programs or software caused deliberately by malicious persons was excluded.

At first instance the Judge held that Tektrol's insurers were not liable for the losses caused by either the virus or the burglary under the terms of the policy. It was an agreed fact that the sender of the virus was a malicious person and the Judge decided that the loss had been caused deliberately even though the virus had not been specifically targeted at or intended to harm Tektrol.

The first instance decision was reversed by the Court of Appeal. The Court held that Clause 7(b)(i) of the policy only covered interferences directed specifically at the computers in question. To cover remote hackers by including them as "malicious persons" would mean adding a different category of persons making a very different kind of attack to those excluded. If the insurer wanted to exclude losses caused by remote hackers indiscriminately sending out viruses, that exclusion needed to be set out in a separate clause with specific wording.

The Court of Appeal showed a considerable amount of sympathy for Tektrol. To quote the judgment, "…it does seem harsh that the extraordinary sequence of misfortune which afflicted Tektrol in this case should be compounded by an unsuccessful legal battle to recover the loss from their so called "all risks" insurers". Whilst this may provide some comfort to policyholders, there is no guarantee of a sympathetic court on every occasion. This case therefore provides a warning that companies should take great care when seeking insurance to cover loss of software, in particular proprietary software.

Ofcom announces that RFID will not be regulated in the UK

RFID (Radio Frequency Identification) is a generic term for technologies that use radio waves to automatically identify objects. An RFID chip is made up of a microchip containing data, and an antenna. RFID chips can be read by specially designed chip readers which are activated whenever the RFID chip is in range. The most often used example of how RFID technology will "change our lives forever" is that it will enable a shopping trolley full of products to be scanned instantly without the need to take anything out from the trolley. It also allowed TopGolf to be created (www.topgolf.co.uk) which, on its own, means the technology is a good thing.

Ofcom is responsible for use of the radio frequency spectrum in the UK. In order to protect existing users of the radio spectrum from interference, it authorises the use of new frequencies by granting licences. It is illegal to use or install radio transmission equipment without holding a valid licence.

In August 2005, Ofcom published draft regulations which confirmed that it would be making the radio spectrum available for the use of RFID equipment (e.g. RFID chips and readers). The draft regulations also confirmed that it would not require users of RFID technology to obtain a licence, so long as the equipment only operated in the 865 – 868 MHz frequency band. In November 2005, Ofcom confirmed the draft regulations in a decision and the licence exemption is now in place.

Is using a wireless network without permission a criminal offence?

In a word, "yes". A man was fined £500 and received a 12-month conditional discharge for using a wireless broadband connection without permission. Reports suggest that the accused was found in a residential area using a laptop to access the wireless broadband connection of a local resident.

No transcript of the case is available, but according to press reports the man was prosecuted for two crimes under sections 125 and 126 of the Communications Act 2003. Section 125(1) makes it an offence to dishonestly obtain an electronic communications service with the intent of avoiding the payment of a charge applicable to the provision of that service. Section 126(1) makes it an offence to possess, with the intention of obtaining an electronic communications service dishonestly, anything which may be used for obtaining an electronic communications service.

Gaining unauthorised access to a computer is an offence under the Computer Misuse Act 1990 (CMA). However, the present wording of the CMA requires "an intent to secure access to any program or data". If a wireless network is only used to obtain access to the Internet, it is arguable that there has been no intent to access programs or data on a computer, as such. This may explain why the prosecution brought charges under the Communications Act in this case.

August

A good month for…

Laughing at Politicians

In a letter emailed to Tory and Lib Dem MPs, Charles Clarke gave Labour's new anti-terror law proposals his firm backing. Unfortunately for Mr Clarke, the word document containing the letter still contained tracked changes which showed the wording of previous drafts. Embarrassingly, the previous drafts appeared to reveal Mr Clarke's doubts about the content of the proposals.

A bad month for…

eBay

eBay received a court summons from the General Optical Council (GOC) for allegedly "aiding and abetting" the sale of contact lenses online without the involvement of a qualified optician. Such conduct is illegal under current legislation. The GOC claimed to have asked eBay to prevent the sale of contact lenses in November 2004 and that eBay had refused to take any action. eBay denied this.

January

February

March

April

May

June

July

August

September

October

November

December

Another peer-to-peer software developer bites the dust

On 5 September 2005 the landmark judgment in *Universal Music Australia v Sharman License Holdings* was handed down by the Federal Court of Australia. The case involved the worldwide peer-to-peer Kazaa software which enabled users to share with each other any material placed in a nominated folder on the users' computers. Other users could then search that folder for any file (including copyright protected music files) and download the file direct from the user.

The claimant music companies accused Sharman (and others involved in the operations of Kazaa) of authorising and sanctioning the illegal copying and distribution of music files. After a long trial, the court agreed with the music companies and held that operators of Kazaa had "authorised" copyright infringements on the file sharing system.

Helpfully, the court set out clear reasoning for this decision. First, the fact that the website advised against sharing of copyright files and made users enter into a licence stating they would not infringe copyright, was not seen as being sufficient because the respondent knew that the system was being used to share copyright files. Second, there was technology available, that the respondent chose not to use, that would have curtailed the sharing of copyright files (e.g file filtering). Third, the respondent's website encouraged users to increase their file sharing, criticised record companies for opposing peer-to-peer file sharing and sponsored a "Kazaa Revolution" campaign which had the effect of making it seem "cool" to ignore copyright laws.

Sharman has been made to introduce filters to prevent infringement or face being closed down. Sharman is also facing vast claims for damages, which are reported to be in the billions of dollars, and a court order to pay 90% of the music companies' legal costs.

This Australian decision has far more relevance in the UK than the US Grokster file sharing case (see page 15). Australian copyright law significantly resembles the UK law. The Australian test of "authorising" copyright infringement is very similar to the test in section 16(2) Copyright Designs and Patents Act 1988, which states that copyright is infringed by a person who does a restricted act without the copyright owner's consent, or "authorises" another to do so. It is therefore likely that if a similar case came to the UK, the courts would use the Australian decision and would be likely to focus on the same issues of control, authorisation and preventative methods.

Despite this ruling, it is unlikely that the Australian (or other) courts will completely shut down networks like Kazaa, as this would unreasonably put an end to legitimate file sharing. However the likely effect of the decision is to significantly decrease the commercial value of such file sharing operations and make illegal file sharing operations more alert to the potential threat of damages and costs.

Oracle is refused a software patent

Oracle invented a means of converting text from SGML (Standard Generalised Markup Language) to another mark-up language (e.g. HTML). In 2002, Oracle filed for a patent. Although the conversion could be done using different methods, Oracle argued that much less human input was required using its method.

The original patent examiner refused to grant Oracle a patent because (essentially) methods for performing mental acts and computer programs as such are not patentable. He decided that Oracle's invention was one or both of these. Oracle requested a hearing to appeal against the patent examiner's decision.

The Hearing Officer ruled against Oracle and therefore the patent was not granted. Oracle had based its arguments on the "little man" test, which allows patents to be awarded for computer programs where the invention would still be new and obvious if the functions of the computer were replaced by a little man doing the same thing.

The hearing officer held that "a little man could never replace the computer in this invention without defeating the main purpose of the invention" and that therefore the little man test could not be applied in this case. The whole point of Oracle's invention was that it was a way of doing something by computer that would take a long time manually.

The hearing office also held that the invention related to a mental act, which was another ground for rejecting it.

Court sentences Demon Internet founder for intercepting emails

The founder of Demon Internet, Cliff Stanford, was fined and given a six month prison sentence after being found guilty of unlawfully intercepting emails.

Mr Stanford resigned as a director of Redbus Interhouse plc after a dispute with the Chairman of the company. Both he and the Chairman had a significant shareholding in the company and Mr Stanford retained his shareholding after he resigned. The prosecution alleged that Mr Stanford wanted to win control of the company and that he required the Chairman to resign.

It was further alleged that Mr Stanford hired a private detective to attempt to gather information which might discredit the Chairman. The prosecution had evidence that a "mirror wall" was set up on Redbus' email server such that all of the Chairman's emails were sent to a hotmail account set up by the private detective. The intercepted emails contained numerous personal details, including bank details, privileged legal documents and business memos.

The Regulation of Investigatory Powers Act 2000 makes it a criminal offence to intentionally intercept any communication in the course of its transmission by means of a public or private telecommunication system. The Judge found Mr Stanford guilty of this offence. Mr Stanford was sentenced to six months in prison and was fined £20,000.

September

A good month for…

Showing that IT companies registered more patents than any other in 2004

This month the Patent Office released its "facts and figures" for 2004 – 2005. The statistics included for 2004 show that IT companies registered more patents than companies from any other industry. The top ten companies listed (in order of the number of patents registered - with the most first) included: Hewlett Packard, NEC, IBM, Samsung, Ericsson, Motorola and Intel.

A bad month for…

Google

IIIR claims to have used the name "Gmail" for an email service for more than 2 years before Google launched Gmail in the UK. It therefore rushed to register GMAIL as a trade mark when Google launched the service. Google entered into lengthy settlement talks with IIIR over the use of "Gmail" in the UK. Such negotiations broke down in October and Google announced that Gmail would be rebranded in the UK to Googlemail.

January

February

March

April

May

June

July

August

September

October

November

December

Citigroup, Domain Names and Instruments of Fraud

The decision in *Global Projects Management v (1) Citigroup Inc and (2) Davies* from October taught two valuable lessons: number one, if you are contemplating a merger that would require or result in any sort of name change, it is worth considering a domain name registration prior to any public announcement; and number two, if you register a domain name which leads people to believe that you are linked to another organisation or person, that is enough to make that domain name a potential "instrument of fraud" which may amount to passing off.

On the day Citicorp and Travellers Group issued a press release stating they were planning to merge, Mr Jim Davies successfully applied to register the domain name *citigroup.co.uk* for an IT security business, Global Projects Management Limited (GPM). GPM had no connection with Citigroup and did not attempt to sell the domain name, but anyone accessing the domain name was automatically taken to the GPM website and emails, possibly confidential and sensitive, sent to the *citigroup.co.uk* address by mistake were held by the GPM system.

Citigroup only became aware of the existence of the domain name in 2003, 5 years after the merger, at which point it wrote to GPM alleging that the registration was an act of passing off and trade mark infringement. GPM issued proceedings claiming damages and other relief for unjustified threats under the Trade Marks Act. Citigroup counterclaimed and sought to have the domain name removed from GPM's ownership and assigned to Citigroup. Citigroup also claimed damages from GPM and Mr Davies.

Citigroup succeeded in an application for summary judgment. It was obvious that the registration was made with knowledge of the press announcement and Citigroup had the requisite reputation in the UK for a passing off action. In addition, there clearly had been an infringement of Citigroup's registered trademarks.

On the face of it, this decision went one step further than the infamous *One in a Million Decision*, which involved cyber-squatters attempting to sell the domain names in question. Here, the defendants were not attempting to sell the *citigroup.co.uk* domain name. However, the defendants were receiving additional traffic to their website as a result of holding the domain name and the Judge was persuaded that the registration of the domain name on the day of merger was not a coincidence.

Although the decision was favourable to the Citigroup, the implicit dangers of confidential email exchange and possible re-direction of Internet traffic, together with the cost of requiring a cyber-squatter to hand over a domain name make it highly desirable to avoid any such situation. This could be avoided by simply applying for the required domain names prior to (or at least at the same time as) any public announcement of a merger or name change generally.

The most unjust court decision of 2005…

After the Indian Ocean tsunami disaster, a number of charity websites collected money online. Mr Cuthbert, a computer consultant, clicked on a banner advertisement which appeared to link to the Disaster Emergency Committee (DEC) appeal website. He then proceeded to input his credit card details and donate £30. However, when he did not receive an email confirmation for his payment, Mr Cuthbert became suspicious and feared he had fallen for a phishing site.

To check and see whether or not he had been the subject of a fraud, Mr Cuthbert tested the website he had been directed to when clicking on the banner advertisement. Unfortunately, in testing the site, he set off the DEC website security systems, and the police were called in.

Mr Cuthbert was charged with committing an offence under section 1 of the Computer Misuse Act, namely the offence of obtaining "unauthorised access to computer material". Mr Cuthbert was found guilty and was given a £400 fine and ordered to pay £600 towards the prosecution's costs. According to press reports, the Judge made the decision with "considerable regret" but stated that "unauthorised access, however praiseworthy the motives, is an offence".

As a result of what appears to be a very harsh and unjust conviction, press reports suggest that Mr Cuthbert has lost his job and has been unable to secure alternative employment.

The DTI publishes the RoHS Regulations

The Directive on the Restriction of the Use of Hazardous Substances in Electrical and Electronic Equipment (RoHS Directive) is one of the two main Directives aimed at increasing "producer responsibility" (the other is the WEEE Directive). The Directives aim to ensure that producers placing products on the market take responsibility for disposing and recycling those products once they have reached the end of their life.

The purpose of the RoHS Directive is to restrict the use of hazardous substances in electrical and electronic equipment that is marketed in the EU. The idea is to minimise the impact on the environment when such equipment is disposed of at the end of its life.

The DTI published the RoHS Regulations on 21 October 2005 (SI 2005/2748) which will come into force on 1 July 2006. The Regulations provide that "a producer shall ensure that new electrical and electronic equipment put on the market on or after 1 July 2006 does not contain hazardous substances". The regulations will therefore apply to relevant products created before 1 July 2006 but not put on the market until after that date.

IT equipment producers will need to ensure that they produce and market products which comply with the Directive and the Regulations. Not complying with the Regulations is a criminal offence which is punishable by a fine of up to £5000 for magistrates' court hearings and an unlimited fine for crown court hearings.

October

A good month for…

Croydon Trading Standards

After an investigation by Croydon Trading Standards, a local man was successfully prosecuted for selling a large number of counterfeit items on eBay. He was sentenced to nine months in prison and was ordered to pay £8000 costs. The Asset Recovery Agency was also successful; the man was required to repay £70,000 to his customers within six months or face a further two years in prison.

A bad month for…

BT Ireland

BT Ireland gave everyone a lesson in PR when it wrote an aggressive letter to the owner of btirelandsucks.com to request that he stop using the domain name. The owner of the website published the letter on his website and the (otherwise little known) gripe site became a news phenomenon. The website owners complaint was that BT had not billed him for three months. The text at the top of the website eloquently told BT Ireland to: "Fix your f**king billing system you muppets!"

January

February

March

April

May

June

July

August

September

October

November

December

The Government wants to transform

In November the Government published its strategy to provide "overall technology leadership" in the delivery of public services, the internal efficiency of governmental organisations and the delivery of technology for government. A timetable for the implementation of the strategy is expected in April 2006. Comments on the strategy, grandly titled *Transformational Government – Enabled by Technology*, were requested by 3 February 2006.

IT service suppliers will be most interested in those parts relating to portfolio management, reliable project delivery and supplier management.

Portfolio management is aimed at providing a more comprehensive overview of the significant IT-enabled projects and operations within the public sector, which it is intended will lead to the creation of more predictable results.

The reliable project delivery strategy involves further measures aimed at managing and controlling IT projects, including: greater scrutiny of the most important government programmes, better management of the transition from policy to practical implementation, development of new IT-enabled project methodology and control tools, closer support for key programmes and mission-critical projects and a continuous improvement approach.

Supplier management is aimed at addressing the perception that the Government is a relatively difficult customer with whom to deal and that its suppliers are unreliable. The strategy envisages the use of agreed performance plans and standardised contracts, service and service boundaries and contracts and service management models. The Government also demonstrates that it recognises the burden placed on individuals and companies of repeatedly providing information to different areas within the public sector and has proposed a new data-sharing model which is a compromise between privacy rights on one hand and higher quality and more efficient services on the other.

The strategy has been welcomed by IT suppliers and, in response to the publication of the strategy, the industry organisation Intellect has created a new Public-Sector Council, intended to create a forum where suppliers can communicate and disseminate their views on various issues as well as communicating with the e-government unit in order to implement the supplier management objectives of the strategy.

More on DoS attacks and the Computer Misuse Act 1990

In February (see page 6) the issue of criminal liability for Denial of Service (DoS) attacks was a hot topic. The issue hit the IT news headlines again in November when a Magistrates' Court Judge effectively held that the Computer Misuse Act 1990 (CMA) could not be used to prosecute those carrying out DoS attacks.

A British teenager who had been sacked sent more than five million emails to his former employer causing its IT systems to crash. He was arrested and charged with making unauthorised modifications to computer material, which is an offence under Section 3 of the CMA.

The Judge dismissed the charges on a point of law before hearing any evidence. He held that the DoS attack could not be said to have made an "unauthorised" modification to computer material, as the server which received the emails was specifically set up for that purpose.

The Judge commented that "the computer world has changed considerably since the [CMA] was passed" and also that "it would appear that Section 3 was enacted to deal with malicious script or code, not with the sending of a vast number of individual authorised emails".

This decision appears to put to bed any suggestion that the CMA could be used against those carrying out DoS attacks. However, the Police and Criminal Evidence Bill (announced in January 2006) proposes amendments to the CMA which would specifically include carrying out a DoS attack as an offence.

.eu Dispute Resolution rules published

The Czech Arbitration Court has been appointed as the body responsible for the resolution of disputes relating to the new .eu domain. Following a consultation in the summer of 2005, it published its dispute resolution rules. The rules appear to be based upon or are otherwise similar to the ICANN Uniform Domain Name Dispute Resolution Policy.

The new dispute resolution rules include the following:

- In the first instance, decisions will be made by a single expert. However, either party to a dispute may request that a three expert panel hears any dispute.
- After a complaint is received, the responding party must respond within 30 days. The expert or expert panel will make its decision within 30 days of receiving the response.
- The default language of proceedings will be the language of the registration agreement for the disputed domain name. However, either party can request that the language of the proceedings be any of the twenty five plus official languages of the EU.
- Any decision made by the expert or the expert panel (e.g. that the domain name is to be transferred) should be implemented by EURid within 30 days.

The section of the Czech Arbitration Court responsible for hearing .eu domain name disputes was up and running from 7 December 2005, when the first applications for .eu domain names were accepted by EURid. It is yet to be seen how well the court will cope with the number of disputes it is expected to hear or, indeed, with the 25 language possibilities.

November

A good month for…

Nominet

In March (see page 9 above), Apple was awarded control of the domain name iTunes.co.uk from Cyberbritain. Cyberbritain applied for a judicial review of Nominet's decision to transfer the domain name. However, in November the Judge dismissed the application, noting that Cyberbritain should have used the appeal process which forms part of Nominet's domain resolution service.

A bad month for…

Sony

Sony's November went from bad to worse as more and more press articles appeared attacking the company, after security researchers detected the use of rootkit technology in digital rights management software used by Sony on its Music CDs. Sony was accused in numerous press articles of issuing malware and class actions were commenced against Sony in some US states.

January

February

March

April

May

June

July

August

September

October

November

December

Controversial Data Retention Directive published

Telecommunications data provides a crucial tool to law enforcement authorities in the fight against serious crime and terrorism. On 14 December 2005 the European Parliament voted to accept revised and final wording for a new directive on the retention of telecommunications data (the "Directive"). The Directive harmonises pan-European rules for the retention of electronic communications data and will require communications service providers to retain traffic and location data, including subscriber and user data, but not the content of any relevant communications. The retained data will be available for detecting, investigating and prosecuting serious crime. The definition of "serious crime" will be determined by the member states.

The Directive provides the following key provisions:

- It introduces a data retention period of 6-24 months, with an option for member states to introduce longer periods where circumstances warrant an extension for a limited period.
- E-mail and Internet telephony data are required to be retained. This includes data relating to unsuccessful call attempts, but this does not need to be retained if the provider does not already retain such data for its own business purposes.
- There is no obligation on member states to reimburse service providers for the costs of such data retention, however member states may choose whether or not to compensate providers.
- The Directive does not regulate the access to, or use of, the retained data. This is has been left for the member states to decide under their national laws (subject to their international legal obligations).

Once the Directive is adopted, member states will have approximately 18 months in which to implement the Directive, although they have the option to defer implementation of the provisions requiring the retention of Internet data for an additional 18 months.

Civil liberties groups are concerned that some member states, such as Poland, may abuse the right to introduce longer data retention periods than those currently set out in the Directive. Poland recently indicated that it wished to introduce retention periods of up to 15 years.

The right of Member States to define "serious crime" has also raised the interest of certain industries, in particular the recording and movie industries. It has already been suggested that access to the retained data should granted for the purpose of investigating other crimes, or even intellectual property infringement. This could lead to an unfortunate position where an instrument brought in as an anti-terrorist measure is used to obtain evidence against file sharers.

Roll up, roll up, get your .eu domain names here…

In March 2005, ICANN approved the appointment of EURid, a not for profit organisation, to manage the new .eu domain names. EURid subsequently announced a launch date for registration of the new .eu domain names of 7 December 2005. For a period of 4 months from the launch date, there was a "sunrise" registration period.

The "sunrise" registration period was made up of two phases, each lasting two months. During phase one (Sunrise I), public bodies and holders of registered Community or national trademarks were able to register domain names. During phase two (Sunrise II) those who are able to register during Sunrise I could continue to register their names, but holders of other rights (e.g. passing off) recognised under community law or the national law of an EU member state were also able to register.

In addition to the usual information required to register a .eu domain name, sunrise applications were required to state the right they were relying on to claim the domain name. Sunrise applications were more costly than the normal .eu applications due to the extra administration costs.

Following the "sunrise" period, registrations began on a first come first served basis with no requirements for rights in domain names applied for (the "Land Rush") on 7 April 2006. Registration of a .eu domain name (whether during the sunrise period or afterwards) is restricted to organisations whose registered office, central administration or principal place of business is within the EU; organisations established in the EU and individuals resident in the EU.

Merry Christmas from the OFT…

In December, the Office of Fair Trading (OFT) published new guidance to companies that sell IT goods and services on the Internet or by phone/mail order. The guidance, available on the OFT's website, has been designed to ensure that such companies comply with the Distance Selling Regulations (DSR) and the Unfair Terms in Consumer Contracts Regulations.

The guidance sets out the obligations placed on retailers in the regulations and also the restrictions placed on the ability of retailers to force consumers to sign up to onerous terms and conditions. Of particular focus are unclear warranty and guarantee terms and other misleading terms and conditions.

A surprisingly large number of Internet retailers fail to comply with the Distance Selling Regulations, in particular by failing to allow consumers the right to return products within the 7 day period required by the Regulations. Some charge "restocking" charges and require consumers to pay the cost of returning goods without making this clear when the purchase is made. Both of these would breach the Regulations.

Usefully, the guidance suggests terms in consumer contracts which the OFT considers will fall foul of the regulations and terms which the OFT recommends that retailers use when drafting their terms and conditions. It is hoped that the guidance will prompt small and medium sized online retailers to become compliant with the regulations.

December

A good month for…

Microsoft

Microsoft confirmed that more than 21,000 counterfeit software products had been removed from the UK eBay website in the three months prior to December. According to Microsoft, over half of the listings removed were for sales of counterfeit Microsoft Windows, while more than a third were fake copies of Microsoft Office.

A bad month for…

the Porn industry

The launch of the .xxx domain name was postponed by ICANN again in December without reason. The postponement led to the press suggesting that the US Government (one of the few governments opposed to the release of the domain) had put pressure on ICANN to delay. Whatever the reason for the postponement, it left the owner of the ICM Registry, Stuart Lawley, who has sunk millions into the project, absolutely furious.

CMS Cameron McKenna LLP is an award-winning, international commercial law firm advising businesses, financial institutions, governments and public sector bodies. Our commitment to the Technology sector is a key hallmark of the firm and has led to us becoming a leading practice across Europe.

Our Technology team comprises 8 partners and more than 30 assistants. We have experience of the full range of legal issues affecting any major IT and telecoms technology project, transaction or dispute. In particular, we have experience of the following specialist areas:

- Hardware procurement;
- Hardware supply and maintenance;
- Systems integration;
- Software licensing and support;
- Software development;
- Facilities management;
- Outsourcing;
- Telecoms and Ofcom regulation;
- Data protection and privacy;
- Freedom of information;
- Databases;
- Software copyright and patents;
- Domain names;
- Parallel trade;
- E-Commerce;
- Website development; and
- Litigation and dispute resolution
  – including mediation and arbitration

For advice on any of the topics covered in this review, or to discuss any technology law issues facing you or your business, please contact the head of the Technology team David Roberts, on 020 7367 3678 or david.roberts@cms-cmck.com. Alternatively, please contact the author, Phillip Carnell, on 020 7367 2430 or phillip.carnell@cms-cmck.com

C/M/S/ Cameron McKenna

Law-Now™

CMS Cameron McKenna's free on-line information service

To register for **Law-Now** on-line go to our home page **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