

UPLOAD-IT - 1 OCTOBER 2008

COMPETITION LAW

- ***Racecourse joint venture is pro-competitive rules High Court – Bookmakers v Amalgamated Racing, High Court...***

The High Court has ruled that the creation of a second distributor in the market for racecourse media rights is pro-competitive rather than anti-competitive. The case was brought by an organisation representing the interests of bookmakers operating licensed betting offices. In the past the betting offices had paid a sole distributor ('S') for the right to broadcast live pictures of horse racing. S then made payments to the racecourses for those media rights. Approximately half of the racecourses, unhappy with the payments they received from S, set up a joint venture creating a new distributor to which they could licence their media rights. Other racecourses continued to licence their media rights to S at a reduced price. However, the racecourses participating in the joint venture licensed their media rights to the new distributor at a higher price and consequently the betting offices had to pay high prices for the services shown in their premises relating to those racecourses.

The betting offices had to provide both distributors' services to their customers. They claimed that the joint venture was anti-competitive as it had the object of fixing prices or restricting competition. The High Court found that the aim of the co-operation by the racecourses had been to sponsor the entry of a new distributor into the market. The object of the agreement between the racecourses had the potential to increase competition in the market rather than restrict competition. The resulting increase in price had not been a consequence of price fixing but the result of the pro-competitive entry of a second distributor into a market formerly occupied by S - a monopoly purchaser of media rights. After the entry of the joint venture into the market, there were two purchasers of those rights which amounted to pro-competitive and not anti-competitive activity.

- ***US Department of Justice investigates Google-Yahoo! advertising deal...***

The US Department of Justice ('DOJ') is investigating the Google-Yahoo! deal that would allow Yahoo! to use Google advertisements beside Internet searches whether or not it had its own advertisements available. The US Association of National Advertisers ('ANA') put its objections to the deal to the DOJ on the basis that the partnership would harm its members' ability to buy advertising cheaply from a range of suppliers. The ANA believes that a Google-Yahoo partnership of this sort will control 90% of the search advertising inventory. A ruling by the DOJ as to whether the deal will harm competition in the online advertising market is expected soon.

- ***A pharmaceutical company's refusal to meet orders was an abuse of its dominant position says ECJ...***

The European Court of Justice ('ECJ') has ruled that the pharmaceutical company GlaxoSmithKline AVE ('GSK' - the Greek subsidiary of GlaxoSmithKline plc) abused its dominant position by refusing to meet ordinary orders from wholesalers who engaged in parallel exports. GSK had supplied the wholesalers with a range of prescription only products for a number of years. The wholesalers then supplied the products in Greece and other EU countries in particular the UK and Germany where prices were higher. GSK stopped supplying the wholesalers for a short period on the basis that the wholesalers' exports were leading to shortages in the Greek market and when it subsequently resumed supplies it restricted the quantities it was prepared to supply.

Following a reference from a Greek court the ECJ considered whether a refusal by a dominant company to meet the full orders of wholesalers, with the objective of preventing parallel trade, amounts to an abuse of dominance contrary to Article 82 of the EC Treaty. The ECJ relied on established case law that showed that the refusal to meet the orders of an existing customer constitutes abuse of dominance under Article 82 where, without objective justification, the conduct is liable to eliminate a trading party as a competitor. However, the ECJ also recognised that the dominant company may in a reasonable and proportionate way counter the threat to its own commercial interests posed by the activities of a wholesaler which wishes to be supplied in one member state with significant quantities of products for parallel export to another member state.

The ECJ concluded that an undertaking which is dominant in the relevant medicinal product market and which, in order to prevent parallel exports to other member states, refuses to meet ordinary orders from wholesalers is abusing its dominant position. However, the ECJ found that it was for the national courts to determine whether the orders by the wholesalers are 'ordinary' in light of both the size of the orders in relation to the requirements of the market in the wholesalers' member state and the previous business relations between the dominant undertaking and the wholesalers in question.

CONTRACTS

- ***Sony entitled to the full value of lost PS2 memory cards rules Court of Appeal - Sony v Cinram Logistics, Court of Appeal...***

The Court of Appeal has ruled that Sony is entitled to recover the wholesale price at which Playstation 2 ('PS2') memory cards were sold to one of its largest customers, Game, after they were lost by a distribution company prior to reaching Game. 17,000 memory cards were stolen whilst in possession of Cinram Logistics ('Cinram'), a provider of warehousing and distribution services to Sony. Cinram admitted liability for breach of contract, bailment and negligence. However, Cinram argued that Sony's damages should be limited to Sony's cost of replacing the lost memory cards rather than the price at which the memory cards were sold to Game.

The Court of Appeal considered whether a manufacturer and seller of goods, who lost them through the fault of another before it could make the delivery and before it was entitled to be paid the price, could recover that price as damages for its loss or whether it was limited to the lower manufacturing cost of replacing the goods unless it could not make good the lost sale to its purchaser. The Court of Appeal ruled that in principle, where there was no issue of remoteness or lack of knowledge of the profit, a seller of goods is entitled to recover the value of the goods if they had been lost as a result of a third party default unless it could be shown that the seller had in fact recovered its profit. The Court of Appeal found that the burden of proof was on Cinram to prove that the profit had been earned by Sony making a substitute or replacement sale rather than Sony to prove that it had not recouped the profit.

- ***Arbitration clause in standard terms and conditions for consumers is unfair rules Technology and Construction Court - Mylcris Builders v Mrs G Buck, Technology and Construction Court...***

The Technology and Construction Court ('Court') has ruled that an arbitration clause was unfair where it was contained in standard terms and conditions entered into with a consumer. Mrs Buck engaged Mylcris Builders ('Mylcris') on Mylcris's standard

terms and conditions to carry out some building work. The standard terms and conditions provided for arbitration in the event of a dispute. A dispute subsequently arose as to whether certain sums were included in the cost estimate and Mylcris served a notice of arbitration on Mrs Buck. Mrs Buck, having been advised by her local trading standards authority, made it clear to Mylcris that she did not want the dispute to be resolved by arbitration but Mylcris proceeded to appoint an arbitrator who made an award in Mylcris's favour. The matter came to the Court when Mylcris sought to enforce the award.

The Court found the arbitrator had not been properly appointed. As the arbitration clause provided no mechanism for the appointment of an arbitrator it was governed by the Arbitration Act 1996 ('1996 Act'). The 1996 Act required that in such circumstances the parties should jointly appoint a sole arbitrator and, in the absence of such a joint appointment, any purported appointment failed. A court could have appointed a sole arbitrator where a failure of appointment occurred but that did not happen here. The Court went on to say that the arbitration clause prevented Mrs Buck from having access to the Court and caused a significant imbalance between the professional builder and Mrs Buck as a lay person. A further element of imbalance arose from the fact that the sums claimed were relatively small (the award was for £5,000) and the arbitrator's fees comparatively high (£2,000).

Although it was not disputed that Mrs Buck had signed the contract, the Court ruled that the requirement of fair and open dealing meant that the arbitration clause and its effects needed to be more fully, clearly and prominently set out than they had been. The impact of the clause would not have been obvious to Mrs Buck, a lay person, and by its inclusion in standard terms and conditions Mylcris, albeit unconsciously, had taken advantage of Mrs Buck's lack of experience and unfamiliarity with such a clause. The Court concluded that the arbitration award was not binding on Mrs Buck and therefore could not be enforced.

Samantha Lloyd, assistant editor of Upload-IT comments: 'Businesses contracting with consumers should be wary of including an arbitration clause in their standard terms and conditions. If such a clause is to be included it will require careful drafting to ensure that the provisions and effect of the clause are made absolutely clear to the consumer in advance of entering into the contract.'

COPYRIGHT AND DATABASE RIGHTS

- ***JK Rowling obtains US injunction preventing release of 'rip-off' Harry Potter encyclopaedia...***

JK Rowling has obtained a permanent injunction in a New York court preventing Stephen Vander Ark ('Ark') and RDR Books ('RDR') from publishing The Harry Potter Lexicon. Ms Rowling had previously supported the Lexicon website run by Ark which catalogued details of the fictional world of Harry Potter. However, she brought the legal action last year to stop Ark and RDR making a financial gain out of publishing an unofficial reference book. Rowling argued that the book took an enormous amount of her work and added virtually no original commentary of its own.

In its defence, Ark and RDR had argued that whilst the Lexicon represented a significant use of copyright material, it was a fair use of the material with little difference from any other novel reference guide. The judge, however, disagreed and found that whilst reference materials could help readers Ark and RDR had gone too far in this case stating: 'Lexicon appropriates too much of Rowling's creative work for its purpose as a reference guide'.

- ***Replicas of Star Wars 'Stormtrooper' costume infringes US copyright rules High Court – Lucasfilm v Andrew Ainsworth, High Court...***

Lucasfilm, the production and licensing companies for the Star Wars series of films, brought an action against Andrew Ainsworth for infringement of UK copyright in the High Court. Mr Ainsworth had made the 'Stormtrooper' helmets and armour for the first Star Wars film shown in 1977. Mr Ainsworth kept the original moulds used to make the helmets and armour and in 2004 he began selling replicas made from the original moulds online. Lucasfilm obtained judgment against Mr Ainsworth in the US court in California for copyright and trademark infringement. The High Court had to consider:

- ◆ whether Mr Ainsworth had infringed UK copyright;
- ◆ whether Lucasfilm was entitled to enforce the US judgment in the UK; and
- ◆ whether Lucasfilm was entitled to bring an action claiming infringement of US copyright in the UK and, if so, was it successful.

The High Court found that Mr Ainsworth had not infringed UK copyright because the helmets and armour were not artistic works in which copyright could subsist. Furthermore, even if the items had been artistic works the High Court found that Mr Ainsworth had a defence under the Copyright, Designs and Patents Act 1988. The High Court also declined to enforce the US judgment as the judge found that Mr Ainsworth was not sufficiently present in the US at the date of commencement of the US proceedings or at any time to allow the US judgment to be enforced in an English court. However, the High Court did agree to consider the US copyright claim.

The High Court concluded that an English court could, and in appropriate cases should, determine questions of infringement of foreign copyright cases. The fact that Mr Ainsworth had challenged the jurisdiction of the US courts in the US case was the most persuasive reason in this case for the High Court to determine the US copyright claim. The High Court held that US copyright existed in the helmets and armour and it had been infringed. A further hearing would be required to decide on the consequences of the ruling. However, both parties have been given leave to appeal the decision.

This High Court ruling means that in principle the English courts can consider questions of infringement of copyright from countries outside the Brussels Convention (as well as, as established by previous case law, within it). Additionally, the High Court has not ruled out the possibility that an English court can also consider the subsistence of foreign copyright. However, it is important to note that in his judgment the judge confirmed that copyright is different from patents and trade marks where it is logical that the courts of the registration of those intellectual property rights should have sole jurisdiction over validity in such cases.

- ***Six people arrested on fraud and copyright charges over file sharing network...***

Six people have been arrested in relation to the OiNK music file-sharing members only network. Alan Ellis, thought to be behind the site which specialised in making pre-release albums available to download unlawfully, was arrested last October. Around the same time Dutch police seized servers in the Netherlands which were believed to have been used by the site. Ellis was charged with conspiracy to defraud whilst five individuals, who were arrested following last year's raids on Ellis and OiNK's servers, have been accused of criminal copyright infringement for uploading material to the site.

- ***Google rewords user agreement for new browser...***

Google has amended its user agreement for its new browser Chrome allowing users to 'retain copyright and other rights' that they already hold in the content they submit or display using the browser. The end user licence agreement originally published claimed 'a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive licence to reproduce, adapt, modify, translate, publish, publically perform, publicly display and distribute any Content which you submit, post or display on or through, the Services.' Google has since said that the claim for such wide-ranging rights was an oversight resulting from the re-use of its Universal Terms of Service.

CYBERCRIME/SECURITY

- ***UK the source of the highest number of spam attacks as attacks quadruple...***

The UK is now the source of the highest number of spam (or unsolicited) emails sent to email accounts according to the results of the latest quarterly spamming index produced by anti-spam software company ClearMyMail. The UK is responsible for 20% of attacks - just a fraction more than the US. The results also showed that on average the number of spam emails blocked per customer had quadrupled since the last quarter - an average of 30,846 was recorded for the quarter to June compared with 8,156 in the previous quarter. Other findings showed that the Royal Bank of Scotland was the favoured target for phishing attacks in the personal-finance industry whilst 97% of all emails sent to an Orange ISP account were spam.

- ***Palin's email account invaded by hackers...***

It has been revealed that the US Republican vice-presidential candidate Sarah Palin's yahoo email account has been hacked into. The attack resulted in screenshots of Palin's messages, inbox, pictures and address book being posted to the Wikileaks whistleblowing site. It is believed that hackers were able to exploit yahoo's password resetting system by obtaining personal information about Palin from public sources which allowed them to defeat security questions and re-set the password to give them access to the account. The hacked account gov.palin@yahoo.com, and gov.sarah@yahoo.com (also owned by Palin), have now been deleted and the FBI and US Secret Service have now begun a formal investigation into the attack. The attack coincides with questions being raised as to whether Palin used her personal email accounts to carry out state business. Under US law, whilst personal emails may be deleted, all emails relating to official government business must be archived and are not permitted to be destroyed.

- ***Hackers target Georgian government for 'botnet' cyber attack...***

Hackers have been working on a botnet to mount cyber attacks against the Georgian government computers. 'Botnets' are networks of hijacked machines that are used to send large amounts of spam (or unsolicited) emails, orchestrated denial of service

attacks, viruses or other cybercriminal activity. Spam emails are being sent to unsuspecting users to trick them into clicking on a fake BBC story about the Georgian president being caught up in a gay scandal. Once a user has clicked on the story they are linked to a malicious server that attempts to infect their computer.

The University of Alabama has tracked the messages to 44 computers, six in Russia and one linked to the Russian Ministry of Education. However Mark Warner, director of computer research and forensics at the university, has said there is no evidence that these attacks are state sponsored. Mr Warner believes that the hackers behind the attacks on Estonia last year are most likely to be responsible for these latest attacks against Georgia. He said: 'The attack is so similar it's almost inconceivable that it's not the same people.'

DATA PROTECTION/PRIVACY/CONFIDENTIALITY

- ***Organisations should stop hiding behind the Data Protection Act says the ICO as 'Stupid Aid Week' highlights common misunderstandings relating to data protection rules...***

The Information Commissioner's Office ('ICO') has appealed to organisations to put a stop to the practice of hiding behind the Data Protection Act unjustifiably when dealing with data requests from individuals. The ICO has revealed that in many cases organisations do not properly think through whether they can respond to enquiries from individuals. The deputy commissioner at the ICO said: 'The Data Protection Act does not impose a blanket ban on the release of personal information. What it does do is require a common sense approach. It should not be used as an excuse by those reluctant to take a balanced decision.'

This call from the ICO coincided with 'Stupid Aid Week' which aims to highlight common misunderstandings including the belief by some organisations that data protection stops them giving out any personal information or prohibits them from dealing with certain types of enquiries. Other common misconceptions relating to the application of the data protection rules include the belief that parents are prohibited from taking photos in schools and insurance companies are prevented from sending out a claim form if requested by someone other than the policy holder. Andy Green, a creativity expert, has launched a guide called 'Overcome stupidity in the world around you'.

- ***Details of data loss relating to 5,000 justice staff emerges more than a year after the blunder...***

Details of the loss of a computer hard drive containing the details of up to 5,000 employees of the National Offender Management Services in England and Wales, including prison staff, in July 2007 have emerged. The data loss, by the private computing firm EDS, was reported to the prison service in July but justice secretary Jack Straw was not informed of the security blunder until recently when a letter about the missing drive was leaked to the News of the World newspaper. Mr Straw has ordered an urgent enquiry into the circumstances and the implications of the data loss and the level of risk involved. He has also commissioned a report into why he was not informed by his department of the problem as soon as they became aware of the issue.

Speaking about the loss the national chairman of the Prison Officers' Association said that: 'It is a breach that we believe could ultimately cost the taxpayer millions and millions of pounds, because, if the information lost is personal and sensitive, it may well mean staff having to move prisons, move homes and relocate their families.' Just last month Upload-IT reported how a memory stick containing the unencrypted

names and dates of birth of every prisoner in England and Wales had been lost by a contractor working for the Home Office. (For more on this case, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2803>.)

- ***Hackers steal personal data from Best Western Hotel chain...***

The personal data of guests of a Best Western Hotel in Berlin were stolen by hackers after a compromised log-in ID permitted access to reservations data for the hotel. The data stolen included addresses, telephone numbers, credit card details and places of employment. The hacker is believed to have bypassed the security software and placed a Trojan virus on one of the hotel's machines. This allowed the hacker to collect the username and password of the next staff member to log in.

Media reports suggested that details of up to 8 million people were exposed as a result of security information being sold by a network operated by the Russian mafia. However, the hotel chain said just ten people had been affected by the security breach. A spokesperson for the hotel chain said: 'The compromised user ID permitted access only to the reservations at a single hotel, and there is no evidence of unauthorised access to data for any other Best Western hotel'. An investigation into the data theft is being undertaken by the hotel in conjunction with the FBI and international authorities.

- ***Sale of a hard drive on eBay containing taxpayers' personal details leads to arrest...***

An arrest has been made by Leicestershire Constabulary after it was discovered that a hard drive sold on eBay for a mere £6.99 contained taxpayers' personal data including bank account information and sort codes. Charnwood Borough Council has promised a review into the data loss and said in a statement: 'We have traced the hard drive and are currently retrieving it. The purchaser is co-operating with Charnwood and has stated that the data has not been distributed to any other parties.'

This is not the first time that personal data has been inadvertently exposed via equipment sold through eBay. Last month, Upload-IT reported how a computer containing the personal bank details of over one million people was sold on eBay for £35. (For more on this case, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2806>.) The security blunders come amidst renewed calls from the Information Commissioner's Office for organisations to integrate privacy protections into all new IT systems to protect individuals.

- ***Virgin signs formal undertaking to comply with the Data Protection Act after losing an unencrypted CD containing customers' personal data...***

Virgin Media Limited ('Virgin') has signed a formal undertaking to comply with the principles of the Data Protection Act after it lost an unencrypted CD containing personal details of over three thousand customers interested in opening a Virgin account in a Carphone Warehouse store. Failure to meet the undertaking is likely to result in further enforcement action by the Information Commissioner's Office ('ICO'). The undertaking was one of the measures imposed by the ICO following the data breach. In addition, Virgin has been ordered to encrypt all portable or mobile devices which store and transmit personal information. It must also ensure that all contracts with third parties that process information on behalf of Virgin include a requirement to use encryption software.

- ***Outrage at government proposals to allow private businesses access to millions of medical records...***

Privacy campaigners have expressed outrage at the government's proposal to allow private businesses to access millions of electronic medical records. The massive computer database containing details of almost all visits by patients to hospitals and GPs is part of a long-delayed scheme to give NHS staff access to computerised medical records. However, the information is also valuable to private businesses carrying out medical research or selling products to the NHS. The government has engaged a private company, Tribal, to carry out a public consultation on secondary uses of NHS data. The proposals could allow patients' postcodes, medical conditions and treatments and in some circumstances their names to be passed on to third parties without the patients' consent.

A spokeswoman from patient pressure group Patient Concern stated: 'We have no idea where this information will end up, and we have no control over it. Even when the data is anonymised, it will be easy to trace back to individuals because the nature of medical data is that it reveals a lot about a person. We have seen endless succession of data losses and breaches, and there is little to reassure anyone that this information would be secure.'

DATA RETENTION

- ***Google bows under EU pressure to discard personal data earlier...***

Google has decided to further limit the amount of time it stores data before it anonymising it from 18 months to 9 months to 'address regulatory concerns and to take another step to improve privacy for users' said Peter Fleisher, Google's global privacy counsel. The move comes following continued pressure from the EU's data protection advisory group, the Article 29 Working Body, over Google's privacy policy after the group published a report in April stating that Google had 'insufficiently explained' why they were storing and processing personal data.

Google claims that it needs the information, such as details about search queries made and the unique PC address of the user, to improve its services and fight threats such as fraud, spam and malicious attacks as well as to assist 'valid legal orders' from law enforcement agencies. However, Google has said respecting users' privacy is 'fundamental to earning and keeping their trust' and that although 'there is a great utility in data...we also believe that limiting the amount and types of data we keep we can improve privacy while continuing to provide a strong user experience'.

DOMAIN NAMES

- ***Opportunist cybersquatters cash in on recent bank mergers...***

Cybersquatters have already seized the opportunity to register numerous domain names for recently merged banks. Domain names for the merged Bank of America/Merrill Lynch and Lloyds TSB/HBOS were amongst the targets with bankofamericamerrilllynch.com and lloydstsbhbos.com being just two of the names acquired. Cybersquatters acquire domain names, usually cheaply, in the hope of selling them to the businesses involved or using them as a medium for pay-per-click advertising. Cybersquatters often use automated software to populate a website with relevant content. An example of such a site is the speculative HSBC/Lehman site which looks like a news site about mergers and market movements but which features Google adverts along the margins. The chief operating officer of NetNames,

the domain name registrar, said: 'The lesson has been there for a while for anyone working in the mergers and acquisitions area that this is a key area to focus on in the due diligence process...One can't wait until after the deal is announced or the product is launched'.

EMPLOYEES

- ***High Court delivers a blow to freelance professional consultants ruling that IR35 applies to IT consultant - Dragonfly Consultancy v The Commissioners for HMRC, High Court...***

The High Court has delivered a blow to freelance professional consultants by ruling that the IR35 rules apply to the services of an IT consultant. John Bessell, the sole worker and director and 50% shareholder of Dragonfly Consulting ('Dragonfly') carried out work almost exclusively for AA, the motoring organisation, for three years. His services were provided by Dragonfly through an agency for IT contractors. HMRC claimed that IR35 applied and that Dragonfly was liable to account for PAYE and NICs. The IR35 rules were introduced in 2000 to prevent individuals avoiding income tax by providing their services through an intermediary, most commonly, a personal service company.

The High Court upheld a decision of the Special Commissioner that IR35 did apply to the arrangements in question and ruled that Dragonfly was liable to account for PAYE and NICs on the payments by the AA. In coming to its decision, that Mr Bussell's relationship with the AA was that of employee and employee, the High Court made the following findings:

- ◆ that the notional contract between Mr Bessell and the AA would not have given Mr Bessell an unqualified right to provide a substitute to perform the services for the AA but would have instead required AA's consent, an arrangement compatible with a contract of employment;
- ◆ that regular appraisals and monitoring of Mr Bessell's work satisfied the test of control – an essential ingredient of a contract of employment;
- ◆ that statements in contractual documents that the parties did not intend to create an employment relationship carried little, if any, weight in the majority of cases; and
- ◆ that there was no such intermediate category of 'worker' between employee and a person in business on his own account under general law – it only exists for limited purposes of defined statutory codes.

John Brazier, the managing director of the Professional Contractors' Group, stated in response to the decision of the High Court: 'This is potentially a massive blow to freelancers throughout the country. This case threatens the long-established defences against IR35; we will be looking at the judgment in very close detail to work out its full implications.'

FREEDOM OF INFORMATION

- ***Authorities may in certain circumstances destroy information after receiving request under FOI says ICO...***

The Information Commissioner's Office ('ICO') has said that authorities may be permitted to delete information that is the subject of a request provided that the information was scheduled to be deleted before the deadline for responding to the request. However, the ICO has confirmed that for an authority habitually to destroy information after a request has been received and then write to the requester saying it no longer has the information would be an offence.

The guidance given by the ICO in its guidelines for authorities on how to treat requests for information under Freedom of Information ('FOI') legislation states: 'You do not have to release the information if it is scheduled to be destroyed under your usual retention and disposal schedules before you are due to respond to the request...If the decision to delete or destroy information was prompted by the request, or if destruction is scheduled for a date later than the 20 working day deadline for responding, this cannot apply...' As a matter of good practice the ICO has recommended that public authorities suspend the destruction of requested information and consider the request in the usual way. This position does not apply to Environmental Information Regulations where authorities are legally obliged to delay the destruction of information whilst it considers the request.

INTERCEPTION OF COMMUNICATIONS

- ***Government requests to intercept data doubles...***

The number of intercept requests from central government authorities increased from 253,557 in 2006 to 519,260 in 2007 reveals a parliamentary report by the interception of communications commissioner, Paul Kennedy. The report states that in 2007 154 of 474 local authorities had used powers under the Regulation of Investigatory Powers Act to make 1,707 requests for communications data compared to 122 in 2006. Kennedy stated that councils used the information to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, prey on the elderly and vulnerable, and fly-tippers. However, despite an increase, it is Kennedy's view that local authorities could still make much more use of their powers to intercept traffic information on emails and phone calls to investigate crime.

IT AND INTERNET USE

- ***Microsoft announces long-term strategy to ease virtualisation...***

Microsoft has announced that it has changed the software licensing and technical support for its server applications as part of its long-term strategy to ease virtualisation. Virtualisation allows businesses to host multiple servers on single hardware appliances and enables them to move applications around to use server space efficiently. Previously businesses were only permitted to move applications from one server to another once every 90 days. Under licence agreements for 41 server applications businesses will now be able to move applications as and when required. Microsoft is also extending its technical support for 31 server applications on virtualisation software from third party suppliers.

- ***US court grants safe harbour to online video site...***

A US court has granted Veoh, an online video site, safe harbour under US copyright laws protecting it from liability for copyright-infringing videos posted by users. The US Digital Millennium Copyright Act ('Act') provides publishers with an exemption, or safe harbour, from its provisions if they are only facilitating another's publication of infringing material and are not actively publishing it themselves. To qualify for safe harbour publishers must also have in place and use procedures for the swift take-down of infringing material they are informed about.

Io, a maker of pornographic films, brought an action against Veoh arguing that Veoh's failure to track repeat infringers disqualified it from the protection of the exemption. Rejecting this argument, the US court found that Veoh operated adequate notice and take-down procedures for alleged infringements and its manual spot checks of videos did not remove the right to safe harbour. The US court also rejected Io's argument that Veoh should reduce or limit its business operations or employ more staff to vet each video uploaded. Such a suggestion was found to be contrary to the Act which 'was intended to facilitate the growth of electronic commerce, not squelch it'.

- ***eBay takes legal action against 'cookie stuffing'...***

eBay has taken legal action in the US against two of its affiliates, Digital Point Solutions ('DPS') and Kessler's Flying Circus ('KFC') for alleged 'cookie stuffing'. eBay only pays its affiliates for advertising its services when a user clicks on the advert and engages in a revenue generating activity on eBay within a certain time period. Such activity is tracked by cookies. A cookie is a file which stores information on an Internet user's computer and allows the user to be recognised by the website.

eBay is accusing DPS and KFC of secretly redirecting web users' computers to eBay so that an eBay cookie would be placed in the user's browser. The activity makes it look as though users have clicked on eBay advertisements thereby wrongly associating future revenue activity, if any, by that user with DPS or KFC. eBay believes that to minimise the chances of detection the affiliates avoided stuffing the same computer twice and did not carry out stuffing in the locations from which eBay runs its affiliate marketing programme. eBay is seeking an injunction against DPS and KFC to prohibit them from engaging in cookie stuffing. eBay is also claiming the return of all of the money DPS and KFC have earned through the alleged scheme and damages.

- ***Website link to old news causes share prices in major US airline to crash ...***

A major US airline, United Airlines, saw its share prices tumble after an old news story reappeared on a list of most popular business stories by Sun-Sentinel and was subsequently indexed by the Google News system. The story, dating back to 2002, told of the airlines' declaration of bankruptcy from which it has since emerged. When the story found its way to the Bloomberg news service, which typically appears on dedicated terminals on trading floors, it caused a sell-off which saw the airline's share price drop 33% within five minutes. However, a denial of the airline's bankruptcy appeared within 25 minutes and Google removed the story as soon as it was notified that it was posted in error. The airline's share price although down from \$12.17 had recovered to \$10.27 by the close of trading.

- ***Online retail market continues to grow but businesses fail to keep up with consumers' increasing expectations...***

The online retail market continues to grow but businesses are failing to resolve logistical and technical problems required to meet the increasing expectations of consumers. Tealeaf, a maker of customer experience and behavioural analysis

software, has reported that 87% of the 2,000 people surveyed who buy online have experienced problems when making purchases online and about four in ten of those abandon transactions or move to a competitor when problems occur. Tealeaf's research has also shown that 84% of web users see no reason why web retail systems shouldn't work first time and stated that: 'Most sites are not meeting those expectations'. In addition, consumers are faced with logistical problems such as how to take delivery of items which will not fit through a letterbox if they are out at work. However, the UK's Interactive Media Retail Group has reported a growth of 15.1% in the online retail market in the last year despite the continuing presence of such technical and logistical issues.

MISLEADING ADVERTISING

- ***ASA bans Vodafone radio advert for delivering a disclaimer too quickly...***

Vodafone has been told by the Advertising Standards Authority ('ASA') not to repeat a radio advert after a disclaimer delivered quickly at the end of the advert was challenged by a listener. The advert for a mobile phone package that included 'unlimited' phone calls ended with the disclaimer: 'Subject to status, availability and connection to 18-month contract. Unlimited calls to landlines or Vodafone Mobiles only, fair-use policy, terms and 60-minute call cap applies.' Vodafone contended that it was usual to summarise qualifications to offers in radio adverts in this way and that the disclaimer had been read by an actress in her normal speaking voice. The ASA, however, found that because the limits to the offer were delivered too quickly the important terms and conditions were not clearly audible. As a result the ASA said the advert could mislead listeners contrary to rule 3 of the CAP (Broadcast) Radio Advertising Standard Code.

TRADE MARKS AND PASSING OFF

- ***New rights for brand owners to challenge company names that are too similar...***

Brand owners now have the right to challenge a company name which is too similar to their trading name under new provisions introduced by the Companies Act 2006 which came into force on 1 October 2008. Previously the right to object to a company name only existed if the company name was 'too like' the name of an existing company which had already been incorporated. Even then any decision to require the other company to change its name was at the discretion of the Secretary of State. Those who had a trade mark (but had not registered a company) had to bring a court action against the registrants for trade mark infringement or 'passing off' or claim that the registration of the company name was an 'instrument of fraud'.

Under the new rules there is no requirement to have a registered company name in order to oppose a company name similar to that of a trade mark or trading name. New adjudicators, based at the Company Names Tribunal at the UK Intellectual Property Office, will decide whether or not a new company registration misleadingly suggests a connection with an existing firm, activity or product. It is hoped that these new laws will protect businesses from opportunistic registrations of variations of company names for financial gain.

- ***Chubb fails to oppose registration of MINIMAX trade mark- Minimax GmbH & Co KG v Chubb Fire, High Court...***

Chubb has failed to oppose the registration of the word 'MINIMAX' as a trade mark in the High Court. Minimax applied to register the word MINIMAX as a trade mark in 2003. In 2005, Minimax successfully applied to revoke two trade marks for the word MINIMAX owned by Chubb Fire ('Chubb') on the basis that there had been no genuine use of the trade marks for an uninterrupted period of five years. The application for Minimax's registration was then opposed by Chubb in 2006 relying on the same evidence as it had relied on in the 2005 proceedings to show it had the relevant goodwill and reputation in the mark.

The High Court allowed Minimax's appeal from the hearing officer and rejected Chubb's opposition to the registration. The High Court found that, in principle, it was possible for a party to have made no real use of a mark for five years but to have retained enough goodwill to succeed in a claim for passing off. The High Court considered that it was difficult to define any minimum threshold of residual goodwill which depended on the facts but highlighted the following factors which may be relevant to determine whether a mark has retained any goodwill:

- ◆ how big was the reputation when use stopped?
- ◆ how lasting in the public eye were the goods or services to which the mark was applied?
- ◆ how, if at all, had the person asserting the existence of the goodwill acted in order to keep the reputation in the public eye?

The High Court ruled that the hearing officer had been wrong to conclude that Chubb's servicing and refilling of existing MINIMAX extinguishers which had been returned to it showed some continued use of the trade mark where there was no supply to the public of any product marked MINIMAX.

UNSOLICITED COMMUNICATIONS

- ***ICO issues Lib Dems with enforcement notice over automated calls...***

The Information Commissioners Office has issued the Liberal Democrats with an enforcement notice after it made unsolicited telephone calls to households across the UK. The calls, which included a message from party leader Nick Clegg to households, were found to constitute direct marketing made without prior consent in breach of the Privacy and Electronic Communications Regulations. The ICO received 26 complaints regarding the calls. Deputy Information Commissioner David Smith said: 'We have previously issued detailed guidance to all major political parties on the subject. Many people find unsolicited automated calls particularly intrusive and annoying so it is important that any organisation making such calls ensures that individuals have given their consent before they are targeted.' A future breach of the enforcement notice by the Liberal Democrats could result in criminal proceedings being brought and fines imposed.