

UPLOAD-IT - 1 SEPTEMBER 2008

COMPETITION LAW

- ***Hearing looms for BA bosses charged with price fixing...***

Four British Airways ('BA') executives suspected of being involved in fixing the price of plane fuel surcharges are due to appear before the City of London Magistrates Court on 24 September. They are accused of having dishonestly agreed with others to make or implement arrangements which directly or indirectly fixed the price for the supply in the UK of passenger air transport services by BA and Virgin Atlantic between July 2004 and April 2006. If convicted of the offence under the Enterprise Act 2002, the men may face prison.

The charges have been brought by the Office of Fair Trading ('OFT'), which also fined BA for the collusion with Virgin Atlantic after Virgin blew the whistle on the arrangements. For more on the fines levied on BA last year, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2115>.

CONTRACTS

- ***easyJet founder takes legal action to prevent the airline competing with his other 'easy' ventures...***

easyJet is facing legal action from a surprising source: its founder, Sir Stelios Haji-loannou. Sir Stelios is seeking to limit the airline's ability to raise revenues from alternative activities which may compete with his other ventures. easyJet was founded by Sir Stelios in 1995. Sir Stelios remains a board director, a 16% shareholder and owns the easyJet name through a separate company, easyGroup IP Licensing. The brand licensing contract contains a rule requiring easyJet to make 75% of its income from 'core activities'.

The dispute centres around the interpretation of 'core activities'. easyJet believes that the activities associated with transporting passengers including additional baggage charges, airport parking and hotels all legitimately fall within the definition of core activities and it is fully compliant with the 75:25 rule. Sir Stelios, however, is concerned that easyJet's additional activities clash with his other 'easy' ventures citing easyJethotels and easyJetholidays as potentially confusing with his own brands easyHotels and easyCruise.

A ruling in Sir Stelios's favour could be severely detrimental to easyJet's business model if it is unable to raise revenues through ancillary services, given the rises in fuel costs.

- ***An unqualified promise to sell is not frustrated by virtue of a supplier's failure to supply, rules the Court of Appeal – CTI Group v Transclear, Court of Appeal...***

The Court of Appeal has ruled that where the failure to supply goods arose under a contract containing an unqualified promise to sell, the seller's obligations are not frustrated. In this case, CTI Group entered into two contracts with Transclear for the purchase of cement to be shipped to Mexico. Transclear's supplier, however, was put under commercial pressure by the operator of a cartel in the Mexican cement market and failed to supply the cement to Transclear.

Transclear claimed that the contracts for delivery had been frustrated because it was commercially impossible for it to perform the contracts without the supply. The doctrine of frustration applies where a supervening event changes the nature of the parties' obligations to something other than that which could have been contemplated by the parties when the contract had been made thus discharging the parties from carrying out their further obligations.

The Court of Appeal decided that the doctrine of frustration would not apply to every event which prevents performance of the contract or simply because performance had become impossible. It ruled that Transclear had a personal obligation to deliver or arrange for the delivery of the cement and therefore it bore the risk of its supplier's failure to perform. The cement was not physically unavailable for shipment nor was it illegal to perform the contract and therefore Transclear's obligations were not frustrated.

Samantha Lloyd, assistant editor of Upload-IT, comments: 'This case highlights how narrowly the doctrine of frustration is applied by the courts. Parties wishing to avoid potential liability for breach should ensure that they provide in the contract for events outside their control by including a well-drafted 'force majeure' clause.'

- ***'No show' clause was not a penalty clause as High Court gives useful guidance as to what's an unenforceable penalty and what's a permitted liquidated damages clause – Tullet Prebon v El-Hajjali, High Court...***

The High Court has ruled that a 'no show' clause in an employment contract was a liquidated damages clause - not a penalty clause - and was therefore enforceable. Tullet had entered into lengthy negotiations regarding the employment of Mr El-Hajjali and finally signed a contract which contained a liquidated damages clause in the event of a 'no show' by El-Hajjali. El-Hajjali subsequently decided to stay in his current job and when Tullet failed to recruit a replacement it sued El-Hajjali on the 'no show' clause.

The High Court rejected El-Hajjali's claim that the 'no show' clause was a penalty clause and unenforceable. The Court found that the clause was a genuine pre-estimate of loss consistent with a liquidated damages clause. The fact that the pre-estimate was not precise and that it might act as a deterrent to persuade the individual not to breach the contract did not necessarily make it a penalty clause. The usual measure of loss would be the cost to the employer of finding and recruiting a replacement (after deducting the costs it would have paid had the new employee joined). However, where a replacement could not be quickly recruited the employer may choose to claim the consequent losses it suffers.

The High Court made some useful comments as to when a clause would be enforceable as liquidated damages rather than be an unenforceable penalty. The Court suggested some leeway to allow it to be enforceable even if the calculation of whether the expected loss was precise. It said a clause should not be regarded as a penalty unless the sum specified was 'extravagant and unconscionable' compared to the likely loss. In fact, where calculating the precise losses would be very difficult, as here, having a liquidated damages clause would be particularly helpful. The Court also placed weight on the fact that the parties had roughly equal bargaining power and Mr El-Hajjali had received legal advice and had been warned of the legal consequences of failing to start work. He had not questioned the clause during the negotiations and so should not do so later without good reason.

- **High Court rules that fraudulent misrepresentations render entire agreement clause unenforceable – Peart Stevenson v Brian Holland, High Court...**

Peart Stevenson ('Peart') terminated a franchise agreement with Brian Holland ('Holland') after Holland had failed to pay monies due. In the legal action that ensued Peart argued that Holland's failure to pay was a repudiatory breach of contract and also that Holland had breached the post-termination covenant in the agreement by competing with Peart and soliciting its custom. Holland counterclaimed on the basis that he had been induced to enter into the franchise agreement by misrepresentations made by Peart and its agents as to the likely turnover and profitability of the business and the low risks associated with becoming a franchisee.

The High Court found that Holland's failure to pay the sums due to Peart was a repudiatory breach of contract and that Peart would normally be entitled to damages. Whilst they found that Holland had carried on business in competition with Peart, he had not solicited any custom and Peart had not suffered any loss from Holland's breach of covenant. However, Holland's counterclaim was upheld. The High Court ruled that Holland was induced to enter into the agreement based on the fraudulent misrepresentations made by Peart and its agents. This being the case, the clause in the agreement which stated that Holland had not relied on any representations by Peart when entering into the agreement was unreasonable in the circumstances and could not be relied upon.

- **No business in the area, no breach of restrictive covenant – Chipsaway International v Errol Kerr, High Court...**

Chipsaway owned rights to and knowhow in a system for filling and restoring damage to the bodywork of cars, and also supplied products used in the system, but did not provide a damage repair service. Instead it franchised its rights to use its name, paints and other products to businessmen in local areas. Kerr, a franchisee, decided not to renew his franchise but continued to carry on his business as a car care centre, including a damage repair service, at the same premises. Chipsaway claimed that Kerr was in breach of the restrictive covenant in the franchise agreement which prohibited him, for the period of 12 months following the termination of the agreement, without Chipsaway's prior written consent, from competing with the business within the area.

The High Court ruled that Kerr's business did not compete with Chipsaway's business as there was no other car centre franchisee within the area with whom he could be said to be competing with. The position would be different if Chipsaway granted a franchise to another operator in the area while the restrictive covenant was still in force. However, the Court found that the key phrase was 'which competes' and referred to competing on the facts as they were – not to the chance that competing might happen in the future if circumstances changed.

COPYRIGHT AND DATABASE RIGHTS

- **British woman ordered to pay £16,000 as the crackdown on file sharing continues...**

A British woman has been ordered to pay £6,000 in damages, plus costs of £10,000, to TopWare Interactive for engaging in the illegal sharing of TopWare's Dream Pinball 3D game which costs only £9 to buy. The case is the first contested victory for TopWare in the UK and is likely to open the floodgates for further claims. Three other suspected unauthorised sharers of the pinball game are awaiting similar hearings and a potential 100 other claims have been threatened. In addition, TopWare's lawyers

have warned that it has court orders for the release of thousands more alleged sharers' identities from Internet service providers. TopWare's lawyers said that the decision demonstrates that 'taking direct steps against infringers is an important and effective weapon in the battle against online piracy'.

Paul Gershlick, editor of Upload-IT, was recently in the media on this case. He says: 'Many employers are not aware of their employees' activities on the Internet, particularly when it comes to playing games and downloading music. Employees need to be more vigilant regarding what their employees are uploading or downloading. They may want to use consider using monitoring technology or banning certain sites, although they also need to be careful not to infringe their staff's privacy rights when they do so. They may be liable for damages awards and their names could appear on court papers and in the media if word gets out that unlawful material has been shared through their Internet connections.'

- ***Ryanair makes its next move in the battle against 'screen-scrapers' by cancelling all tickets bought from aggregators sites...***

Ryanair has made an interesting move in its battle against 'screen-scrapers' by announcing that it will refuse to honour tickets bought from aggregators sites. Screen scraping occurs when a website extracts data from other sites before using that data for its own use, such as offering for sale flights from other operators. Ryanair opposes screen scraping because it says consumers are misled into paying 'handling charges' for Ryanair's flights when they could purchase the same flights with no handling charge on its site.

Last month, Upload-IT reported how Ryanair had obtained an order from a German court preventing Vtours from using information from Ryanair's site to sell flights to Vtours customers. (For more on this case, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2741>.) However, Ryanair has said that it believes that cancelling tickets sold through screen-scraping websites will be a quicker and more effective way of discouraging such activity than legal action through the courts. Meanwhile, Ryanair is also looking into technological solutions with software developers to prevent its sites from being scraped in the first place.

- ***Bratz sellers ordered to pay Barbie rights owners £22m in damages...***

The makers of Bratz dolls, MGA Entertainment, has been ordered to pay damages of at least US\$40m (£22m) in a copyright case brought against it by Mattel, which owns the rights in Barbie. Mattel claimed that the creator of the Bratz dolls, Carter Bryant, had come up with the name and design for the urban fashion dolls while under contract with Mattel, entitling Mattel to the intellectual property rights. MGA argued that the idea for the dolls had come to Mr Bryant during a gap between his two working for Mattel and that MGA had built the value of the dolls with its own additions, branding and packaging. The victory for Mattel is timely as Barbie has been losing out on market share to Bratz. However, Mattel had wanted a lot more – it had claimed US\$2bn.

- ***Symantec obtains record settlement from British counterfeit software dealer...***

Symantec, a security software provider, has reported its biggest settlement in Europe for copyright infringement after agreeing that a British dealer in counterfeit software should pay it damages of £700,000. It also obtained a court order against Nusoft Trading and Robert Waterman barring them from any future dealing in counterfeit Symantec software. A Symantec spokesperson said, 'While the amount of damages is

certainly significant, more importantly, our goal was to put a stop to this operation's dealings in counterfeit Symantec software and to protect any unsuspecting users from using fraudulent security software.'

- ***US appeals court rules that open-source licences can be protected by copyright law...***

The US federal appeals court ('Court of Appeal') has ruled that open-source licences can be protected by copyright law even where the software is given away for free. Open-source licences are designed to allow for free distribution and modification of software as a method of creative collaboration whereby computer programmers make changes and improvements to the software. In this case it was agreed that the software developer was the copyright owner of the software and that the commercial developer had copied and modified parts of the software. However, the Court of Appeal had to decide whether the commercial developer's breach of the software licence was i) an infringement of the software developers copyright; or ii) merely a breach of contract. The distinction is important when considering the remedies available for breach.

Professor Larry Lessig of Stanford Law summarised the decision made by the Court: 'In non-technical terms, the Court has held that free licences set conditions on the use of copyrighted work. When you violate the condition, the licence disappears, meaning you're simply a copyright infringer.'

Although the decision of the Court is specific to US law and the interpretation of each open source licence will depend on the wording of its provisions, the decision is significant for businesses which rely on open source software licences. If those companies had lost their ability to enforce their right under copyright law they may have been reluctant to develop the software.

CYBERCRIME/SECURITY

- ***Cybercriminals run riot in virtual worlds as they become the new playground for money laundering and data theft...***

Cybercriminals have found a new playground for hiding their criminal activity - virtual worlds. The in-game economies of virtual worlds are being manipulated by criminals who hide illegal profits through the exchange of virtual currencies and then convert it into real money. Virtual worlds are also being used to steal private data to aid fraudulent activity. These findings are revealed in a paper produced by McAfee, a web security firm. Users are also being warned to beware of phishing and spam messages tempting users to malicious sites promising 'free' games. 'Phishing' is the fraudulent practice of sending emails purporting to be from reputable businesses in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

DATA PROTECTION/PRIVACY/CONFIDENTIALITY

- ***Microsoft promises privacy protections that will automatically wipe all trace of activity in new Internet browser...***

Microsoft has revealed that Internet Explorer (IE) 8, which is currently being prepared for release, will include a new browsing mode called InPrivate to strengthen privacy protections. The InPrivate mode will allow users to control what information relating to their use of the Internet is stored and published by their browser. Users

will be able to prevent their browser from saving details of their browsing history and from storing any cookies received.

Cookies, in particular, are seen as a major privacy threat to users. They are text files sent from a web server to users' computers, where they are stored on the hard drive and used to 'remember' the visitor next time they visit the site.

Whilst users can currently delete their browsing history and cookies after they have finished using the Internet, the new software will prevent the information being stored in the first place. IE8 is tipped to provide significant reassurance to those users accessing the Internet through a shared or public PC, as information submitted during their session - such as passwords, form data, addresses in the address bar and search queries - will not be traceable.

- ***International proposals to extend customs' powers to searching laptops, iPods and mobiles revealed...***

International travellers could find that their laptops, mobiles and iPods are read, copied and retained by customs authorities, if international plans proposed by Japan and the US get the go-ahead. Consultation papers published by an Australian trade body, the Australian Digital Alliance, has revealed international proposals to extend customs' powers to search, seize and destroy material that infringed copyright and the facilities to produce copies under a new global Anti-Counterfeiting Trade Agreement ('ACTA'). Other proposals include criminalising infringements and subjecting infringers to higher fines and claims for damages.

The executive director of the ADA was reported to have said, 'One of the worse case scenarios was this idea that you might be able to search someone's laptop or iPod for infringing content at the border or at the airport.' A UK association of Internet service providers has voiced its concerns that to allow border authorities to read, copy and retain files could be breaching an individual's right to privacy. Japan and the US are keen to finalise the ACTA by the end of this year.

- ***New Government data security blunder as contractor loses memory stick containing details of every prisoner in England and Wales...***

A memory stick containing the unencrypted names and dates of birth of every prisoner in England and Wales - a total of 84,000 individuals - has been lost by a contractor working for the Home Office, PA Consulting. The data had been provided to PA as part of a contract to manage prolific and priority offenders. The data included personal details of 33,000 individuals with six or more recordable convictions in the past 12 months and of 10,000 prolific and priority offenders. Some data included addresses and expected dates of release.

The Deputy Commissioner at the Information Commissioner's Office, David Smith, expressed his concern over this latest security blunder. He said: 'It is deeply worrying that after a number of major data losses and the publication of two Government reports on high profile breaches of the Data Protection Act, more personal information has been reported lost.' A full investigation is being carried out by the Home Office and the transfer of data to PA has been suspended. Some of the data lost is sensitive personal data - a special type of data that needs special safeguards - as it contained details of the individuals' criminal offences.

Meanwhile, the BBC has reported the theft of one laptop and a number of memory sticks containing the names, addresses and mobile phone numbers of children. The equipment was stolen from a van belonging to an independent production company working for CBBC.

- ***Foreign office reports data losses relating to 188 individuals...***

The Foreign and Commonwealth Office ('FCO') has reported the loss of personal data relating to 188 individuals in five separate incidents over the last year. Unauthorised disclosure by a contractor resulted in the personal details of around 50 people entering the public domain in May 2007; and 70 people's names and addresses, dates of birth and family details were lost in September 2007 from 'an inadequately protected PC from outside secured Government premises'.

In addition to the data losses identified in the FCO report, the FCO was investigated by the Information Commissioner's Office – the UK's data protection regulatory – after details of 50,000 visa applicants had been made available to visitors to a FCO run website in November 2007. As a consequence of the investigation, the FCO signed a formal undertaking to comply with the principles of the Data Protection Act.

- ***MoJ reveals more data losses in annual report...***

The Ministry of Justice has lost the personal details of 45,000 people in the last financial year, it has admitted in its annual resources report. Data loss incidents contributing to this figure include mislaid memory sticks and inadequately protected laptops and the loss of personal data held on computer disks. The police were notified of six of the nine data losses but of the 45,000 people affected only 15,000 were told of data losses affecting them. The MoJ defended its decision to inform just a small number of those concerned, stating that it carried a risk assessment for each incident to decide who should be notified. The lost data included the names, dates of birth, National Insurance numbers, addresses and offence details of thousands of people who had failed to pay fines.

- ***One million bank customers' details sold for £35 on eBay...***

A bidder got more than he bargained for when he purchased a computer for £35 on eBay – it contained the personal bank details of over one million people. The computer held details of customers or potential customers of Royal Bank of Scotland, American Express and NatWest including their bank account information, names, addresses, phone numbers, signatures and mothers' maiden names. In the wrong hands, the extent of the information could have been used to steal identities and commit fraud. Fortunately, in this case, it had been found by an IT expert and he did not misuse the data.

The computer had belonged to Graphic Data, which digitally archives paper-based information. It was reportedly 'inappropriately sold on via a third party' – thought to be an ex-employee of Graphic Data – and a second computer is also missing. Investigations are ongoing into how the computer was removed from one of Graphic Data's secure locations.

The Financial Services Authority has the power to fine companies for this sort of data breach including for breaches committed by the firms they outsource services to. Two year ago, it fined Nationwide Building Society £1m after a laptop with customer data had been stolen.

DATA RETENTION

- ***Government publishes consultation on draft regulations requiring retention of Internet data...***

The Government has commenced a consultation on draft Regulations that will require providers of electronic communications services ('CSPs') to retain Internet related data. CSPs will be subject to similar data retention obligations that were imposed on

telephone companies from last October under the Data Retention (EC Directive) Regulations 2007 ('2007 Regulations') in relation to fixed and mobile telephone data. Since last year's laws came into force, telephone companies have been required to retain the data surrounding every phone call made in this country for 12 months. The new Regulations will replace the 2007 Regulations to cover both non-Internet and Internet data.

Currently, CSPs can opt to retain Internet-related data under a voluntary Code of Practice which requires the data to be held for six months. Under the draft Regulations, the retention period will be increased to 12 months from the date of a communication. However, the Secretary of State can vary that period for individual CSPs to anything between six and 24 months by serving them with written notice of the variation. Information to be stored will include details of Internet use, such as the time of its use, its instigating Internet protocol address and the destination email addresses or website addresses visited, but CSPs will not be required to store the content of any communication. The draft Regulations will also require the retention of data relating to unsuccessful call attempts that are stored or logged in the UK. This will be of concern to privacy groups, which have argued that law enforcement agencies should not be allowed to use that data because of the risk of implicating innocent diallers in police enquiries.

The draft Regulations will not apply to a CSP to the extent that the data is already retained by another UK CSP. The aim is to obtain full retention of all data generated by the UK whilst avoiding duplication of retained data. However, the proposed provisions contain considerable room for error on the part of CSPs and it appears that they will need to carry out a legal assessment of whether or not the draft Regulations apply to them.

The communications industry has always argued that the Government has not made a proper business case for the extension of the retention period for Internet-related data from six to 12 months. Whether the extension envisaged in the draft Regulations justifies the increased cost of retention incurred by CSPs is debatable. The Secretary of State will retain the discretion given under the 2007 Regulations to reimburse any additional expenses incurred by providers in complying with the draft Regulations, provided that those expenses have been notified to the Secretary of State and agreed in advance. The concern for CSPs will, therefore, be the discretionary nature of the reimbursement.

DEFAMATION

- ***Libellous email drifts University into rough waters...***

The University of Salford has found itself in rough waters after Dr Tom McMaster, a lecturer, took legal action following an email from the University's finance director, Ray Corner, accusing Dr McMaster of submitting a fraudulent expense claim. The University had previously given Dr McMaster permission to sale his boat to a conference in Galway rather than flying, but his expense claim for £180 was subsequently rejected. When Dr McMaster queried the rejection, Mr Corner responded that 'clearly the original claim was an attempted fraud and appropriately rejected. Those who submitted and certified it should be ashamed of themselves.' Mr Corner copied in four of Dr McMaster's colleagues to the reply. By sending it to other people as well, Mr Corner opened the door to a libel claim against the University, his employer. The University's application to have the case struck out as frivolous was rejected by the High Court and the University settled the claim out of court for £10,000. Reports suggest that the University had to pay about £100,000 in legal fees.

Paul Gershlick, editor of Upload-IT, comments: 'This case shows how careful staff need to be. Or one misjudged email could end up costing an organisation tens of thousands of pounds. Staff should be appropriately trained on the dangers of email and Internet misuse, and employees should be given clear, well-drafted policies.'

- ***High court gives guidance on how defamation law applies to bulletin board communications – Smith v ADVFN, High Court...***

The High Court has given some helpful guidance as to how defamation law applies to the Internet and in particular to bulletin board communications. Libel and slander are the two limbs of defamation - libel being the publication in permanent form of a defamatory statement and slander being its publication in transitory form. In this case, the High Court said that it was necessary to take into account the nature of bulletin board communications. It was characteristic of bulletin board communications to be:

- ◆ Read by relatively few people, most of whom would share an interest in the subject matter;
- ◆ Rather like contributions to a casual conversation which people simply noted before moving on;
- ◆ Often uninhibited, casual and ill-thought out;
- ◆ Used by individuals who often hide their identities by using pseudonyms.

Given these features the judge commented that, in the context of defamation law, communications of this kind were much more like slander than the usual more permanent kind of communications found in libel claims.

The Judge went on to say that in the case of bulletin board communications it was often obvious to casual observers that people were just saying 'the first thing that comes into their heads and reacting in the heat of the moment' and that the remarks were often not intended to be serious or to be taken as such. The judge also emphasised that account could be taken of the fact that bulletin postings were not made in a vacuum and readers of the thread could put the comments into context.

The Judge's comments are interesting because they provide general guidance on both how the courts may consider claims relating to alleged defamatory postings on bulletin boards and how to assess whether a particular comment on a bulletin board is defamatory. The distinction between slander and libel is important because, with slander, the claimant has to prove he has suffered some actual loss, but this is not necessary for libel actions. Until this case, it had usually been thought that web postings were libel rather than slander.

IT AND INTERNET USE

- ***YouTube criticised for failing to do enough to police the 'dark side' of the web...***

YouTube – the popular video-sharing site - has been criticised in a Parliamentary select committee report for failing to do enough to police the 'dark side' of the web. The Culture, Media and Sport select committee has also condemned the 'lax' approach taken by some websites in respect of the removal of child abuse images. The industry standard for taking down illegal content is 24 hours. The committee has

called for sites hosting user generated content to proactively review material as standard practice.

Google, the owner of YouTube, has defended its strict rules and system of user regulation which enables users to report inappropriate content to its review team 24 hours a day. A Google spokesman stated that YouTube's current practice was the most effective way of ensuring that illegal videos are taken down quickly given the volume of content uploaded. Although the committee accepted that it may be unrealistic for websites like YouTube to vet every video before it is posted online, it was not happy with the process of removing clips only after they have been viewed and reported. It has also recommended that a new body be set up to monitor uploaded material and protect children from harmful content on the Internet.

Pre-screening raises a concern for Internet service providers and website operators of potential liability for defamation or other claims relating to the content. They are less likely to be held legally responsible for illegal material if they have not seen it. To counteract these fears, the committee's report recommends that Ofcom or the Government clarifies when Internet service providers would be liable under the E-Commerce Directive for content that they host or enable access to. The committee commented: 'It would be perverse if the law were to make such sites more vulnerable for trying to offer protection to consumers.'

The report also called for regulation of video games. It is unclear yet whether the British Board of Film Classification will give age ratings to the games, or whether the games industry will create a voluntary code.

In an interview live on Sky News, Mark Weston, head of Commercial/IP/IT at Matthew Arnold & Baldwin, commented that the committee report is likely to raise some serious concerns with Google: 'Statistics show that every minute there are 10 hours' worth of footage uploaded on to YouTube. There are companies that already do pre-screen everything, for example MySpace have hundreds of people in their offices over in the US pre-screening everything that goes up, but of course MySpace isn't primarily a video hosting site whereas YouTube is.'

- ***ISP censured by US regulator for filtering P2P traffic...***

Comcast, the Internet service provider ('ISP'), has been censured by the Federal Communications Commission ('FCC'), the US regulator, for filtering traffic on peer-to-peer ('P2P') networks and so treating them differently to other Internet traffic. Although Comcast denied obstructing downloads via P2P networks it admitted it practised 'very limited management' of P2P uploads. The majority of the FCC Commissioners slammed Comcast's behaviour as unacceptable and ordered it to change the way that it operates its network.

The decision supports the principle of net neutrality - the term given to the current Internet climate where users obtain equal access to all information without differing speeds of access - which has been the focus of much debate by policy makers and telecoms companies. As recognised by one of the Commissioners, 'Consumers have come to expect - and will continue to demand - the open and neutral character that has always been the hallmark of the Internet.'

- ***NHS faces unprecedented £700m legal action as MP brands IT programme as hopelessly flawed...***

Reports that Fujitsu is threatening legal action against the Department of Health has prompted Liberal Democrat Shadow Health Secretary, Norman Lamb, to brand the National Programme for IT as hopelessly flawed. Fujitsu is thought to be seeking £700m in damages following the termination of its £1bn contract as the local service

provider in the south of England. Mr Lamb has been quoted as saying the IT programme was a 'centrally-imposed project that has not been properly thought through from the start and was never subjected to a proper cost benefit analysis'. 23 leading academics have called for an independent review of the scheme.

- ***Two thirds of UK homes now online...***

Two thirds of UK households now have Internet access, up by 1.2 million since 2007. There are now about 16.5 million households online. These figures come from The Office for National Statistics. However, charities have criticised the Government and the industry for failing to assist older people to get online, as 7 million people over 65 have never used the Internet.

JURISDICTION

- ***Government signs up to new rules on EU cross-border contract laws...***

The Government has signed up to the new EU rules that deal with the issue of which country's laws apply in cross-border situations. The new rules are called the Rome I Regulation ('Regulation'). The Regulation, which will come into effect in December 2009, is set to replace the Rome Convention of 1980 ('Convention') which currently determines how parties in different countries should settle disputes over which country's laws apply. The basic principle of the Convention is that two parties can choose which countries' law will govern their dealings, although this is subject to consumers also not losing the protection of any mandatory provisions protecting them in their home country.

In a recent consultation, the Government had recommended that the UK opts into the Regulation to avoid losing the benefit currently provided by the Convention and also to avoid the need to maintain two separate systems which would increase the legal complexity for businesses. The majority of participants who responded to the Government's consultation backed signing up to the Regulation.

MISLEADING ADVERTISING

- ***Apple receives slap on the wrist for misleading iPhone advert...***

The Advertising Standards Authority ('ASA') has ruled that Apple's television advert which claimed that 'all parts of the Internet are on the iPhone' gave a misleading impression of the Internet capabilities of the iPhone. The iPhone does not support Flash or Java, two software programs that form part of many web pages to display graphics and animations. The iPhone uses a web browser called Safari. As a result, web pages viewed may look different when viewed using the iPhone compared to other browsers.

Apple tried to argue that its claim in the advertisement related to the availability of web pages rather than their appearance, but the ASA took a different view and upheld its ruling that the advert misled customers. The ASA has ruled that the advert must not be aired again in its current form.

MISLEADING SELLING

- ***Draft Regulations published in respect of contracts made in consumers' homes, places of work and elsewhere...***

Draft Regulations that are set to replace the Consumer Protection (Cancellation of Contracts Concluded away from Business Premises) Regulations 1987 have been published. The draft Cancellation of Contracts made in a Consumer's Home or Place of Work etc. Regulations 2008, which are expected to come into force on 1 October, would:

- ◆ Extend the cooling-off period and right to cancel contracts entered into during solicited visits from traders made at a consumer or another's home or place of work or on an excursion - as well as contracts made during unsolicited visits at those places;
- ◆ Set the threshold value caught by these contracts to those with a total payment value of £35;
- ◆ Require a seven day cooling off period from receipt of the notice of the right to cancel;
- ◆ Specify that the notice of the right to cancel must be prominently displayed in the contract and include a statement that payment may be required if the consumer requests performance of the contract before the expiry of the cooling off period and the contract is subsequently cancelled;
- ◆ Provide that any request to commence performance of the contract prior to the expiry of the cooling off period should be recorded in writing;
- ◆ Make a failure to include all required information in a notice an offence; and
- ◆ Allow for the automatic cancellation of a related credit agreement where a cancellation notice is served on a trader.

- ***Trading Standards1 Rogue Traders 0, as first enforcement order is made under the new Consumer Protection from Unfair Trading Regulations 2008...***

The first enforcement order under the Consumer Protection from Unfair Trading Regulations 2008 ('2008 Regulations') has been awarded. The order was obtained by the trading standards department of Wiltshire County Council with the support of the Office of Fair Trading ('OFT') in Salisbury County Court against two handymen. Trading standards had received a number of complaints against the father and son team relating to their aggressive behaviour and poor quality work. The order prohibits the Stockwells from breaching a number of provisions in the 2008 Regulations including not to:

- ◆ act in a misleading manner by presenting false information or presenting it in a way likely to deceive the customer;
- ◆ make contracts away from business premises without providing the customer with written notice of their cancellation rights;
- ◆ act in an aggressive manner either in attempting to get the consumer to enter into the contract or by obtaining payment; and

- ◆ act without professional diligence.

If the Stockwells breach the order they could be found to be in contempt of court and face a fine or imprisonment or both. Gareth Thomas, the Consumer Affairs Minister, said: 'The Government introduced these new regulations to enable Trading Standards and the OFT to crack down on rogue traders...Life is going to get tougher for the small minority of rogue traders who subject customers to aggressive commercial practices to make a sale.'

TRADE MARKS AND PASSING OFF

- ***Dell's controversial 'cloud computing' trade mark application fails at the last hurdle...***

Dell's trade mark application to register the term 'cloud computing' for remote computing services and hardware has been rejected by the US Patent and Trade Mark Office ('USPTO') in a late stage in the application process. The trade mark application was made by Dell in March 2007 to protect its brand 'Cloud Computing Solution' but the controversy surrounding the term's generic nature prompted the USPTO to reconsider the application.

Cloud computing is a term used to describe remote computing applications. The USPTO rejected the application on the basis that 'the applied-for-mark merely describes a feature and characteristic of applicant's services' and therefore not appropriate for trade mark registration 'because the average purchaser of services, when encountering the mark in connection with the services, would immediately perceive a feature of the services'. The USPTO also found that the term was generic in connection with the identified services as it was in general use in the computer industry.

- ***Belgian court backs eBay in its battle to fend off claims relating to counterfeit sales...***

A Belgian court has rejected L'Oréal's claims that eBay does not do enough to prevent the sale of counterfeit goods on its platform. eBay's verified rights owner scheme ('VeRO') enables brand owners to ask eBay to remove counterfeit goods from auction but eBay does not pre-screen sales of branded items. In a statement, eBay said: 'This is the second successful court ruling in a row for eBay, both supporting our view that controlling prices and distribution reduces consumer choice...eBay provides a vibrant and trusted marketplace that gives European consumers a good deal. We work to tackle the menace of counterfeit through action and co-operation with rights owners.'

eBay has recently faced a barrage of claims relating to counterfeit sales from luxury brands in courts across Europe and in the US. Upload-IT reported last month that the French courts had ordered eBay to pay €40 million to Louis Vuitton Moët Hennessy. In contrast, the US courts rejected Tiffany's claims that eBay's anti-counterfeiting actions were inadequate. For more on this article, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2762>. Tiffany intends to appeal the US decision.

UNSOLICITED COMMUNICATIONS

- ***Phone regulator issues £200,000 fine to phone scammer...***

Jack Barnard Telecom Services of Epping has been slapped with a £200,000 fine from Phonepayplus for breaching its code of practice. The service provider used automated calling equipment to make unsolicited telephone calls of a man's voice saying 'Hello, hello, can you hear me?' which prompted recipients to call back. The recipients, however, were unaware that the number they were calling was a 070 higher rate number, where they were paying at least 50p per minute for the privilege.

Phonepayplus, the regulatory body for all premium rate charged telecommunications, has said that this is the second highest fine it has issued since an increase in the maximum fine available. A £250,000 was levied on Opera Telecom after viewers lost an estimated £20m on GMTV's phone-in quizzes.