

Legal Developments



Commercial/IP/IT communications – April 2009

COMPETITION LAW

Complaints about bus services spark OFT inquiry...

Regular complaints to the Office of Fair Trading ('OFT') about bus prices, service levels and a perceived lack of competition between the operators has sparked an OFT investigation into local bus services. After a number of takeovers in the sector, nearly two thirds of the country's bus services are controlled by five operators: Arriva, Go-Ahead, Stagecoach, First Group and National Express. The OFT inquiry will examine the impact of this concentration in the market on prices and services and why, even where there is competition, the service providers have failed to deliver improvements in local bus services. The study will see the OFT collaborate with local authorities, bus operators and the government to obtain information to test these issues.

CONTRACTS

Franchisee did breach restrictive covenant despite no business in the area, says Court of Appeal - Chipsaway International v Errol Kerr, Court of Appeal...

The Court of Appeal has ruled that a former franchisee who operated his own car service business following the termination of a franchise agreement was acting in breach of restrictive covenant, despite the fact that the franchisor had no other businesses in that territory.

Chipsaway owned rights to and know-how in a system for filling and restoring damage to the bodywork of cars, and also supplied products used in the system. It franchised rights to use its name, paints and other products to businessmen in local areas. Kerr, a franchisee, decided not to renew his franchise agreement 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, however, ruled that Kerr's business did not compete with Chipsaway's business as there was no other car care centre franchisee within the area with whom he could be said to be competing. The High Court thought that the position would be different if Chipsaway had granted a franchise to another operator in the area while the restrictive covenant was still in force.

The Court of Appeal took a different view. It found that the commercial purpose of the restrictive covenant was to stop Kerr from carrying on the business in the area to allow Chipsaway 12 months' breathing space to find a new franchisee. The fact that Chipsaway did not look for a new franchisee was irrelevant as the meaning of the covenant was not dependent on there being a new franchisee in the territory.

Courts should interpret contracts to give them effect as opposed to rendering them void, says Court of Appeal – Anglo Continental Educational Group v Capital Homes, Court of Appeal...

The Court of Appeal has confirmed that courts should try to interpret poorly written contracts to give them effect, as opposed to interpreting them in such a way which would render them void. The Court made its ruling in respect of a dispute over a property deal where the buyer and seller subsequently disagreed over the meaning of the contract for the sale of two properties. The sale price was stated to be £862,000 minus fees payable for the release of restrictive covenants (such fees being a discount on the sale price). The seller argued that discount to the price should not be applied because the covenant fees did not arise at the time of sale – the buyer having proceeded with the sale without having the necessary planning permission to obtain the release. The buyer believed it should receive the discount because it would have to pay the costs eventually.

The Court of Appeal ruled that courts should always try to declare a contract effective by choosing an interpretation that is the likely outcome of the parties' agreement, rather than one that seems improbable. In this case, as the buyer would have to pay the covenant fees eventually, whether before or after completion of the sale, the discount should be paid.

Samantha Lloyd, assistant editor of Upload-IT, comments: 'The decision of the Court of Appeal should act as a sharp reminder that courts will do their utmost to interpret a contract to give it force rather than to render it void. However, to rely on a court interpretation is dangerous as it may not be consistent with either of the parties' original intentions. There can be no substitute for ensuring that a contract is clearly and well drafted by a specialist lawyer at the outset. Contractual disputes are costly as well as inherently unpredictable.'

Warning - statutory interest is payable for late payment of invoices even if those invoices contain mistakes - Ruttle Plant Hire v Secretary of State for Environment, Food and Rural Affairs, Court of Appeal...

Statutory interest arising under the Late Payment of Commercial Debts (Interest) Act 1998 for failure to pay on time will still be payable even if the invoices to which it relates contain mistakes. This was according to the Court of Appeal's decision in this case. Ruttle had contracted with DEFRA to provide cleansing and decontamination services. It submitted numerous invoices to DEFRA between August 2000 and January 2005, some of which were incorrect as a result of the wrong hourly rate being used in the calculations. A final account was submitted by Ruttle in Spring 2007 which showed the correct sums due under the invoice.

Notwithstanding the mistakes in the original invoices, the Court of Appeal ruled that the statutory interest rate applied. The 1998 Act did not require an invoice to be perfect before interest could apply. DEFRA could have worked out the correct amount due from the underlying documentation submitted with the invoices and paid that. The Court of Appeal ruled that a paying party should check invoices on receipt and pay any amount which was undoubtedly due. In addition, it should explain to the supplier why it is not paying more and request an explanation of the sums outstanding.

The decision highlights the risk of statutory interest being imposed if a paying party simply withholds payment until a correct invoice is presented. Businesses should carefully consider all invoices received and ensure that they make prompt payment of sums due as well as actively challenging those in dispute.

COPYRIGHT AND DATABASE RIGHTS

Dispute over licence leads to music videos being pulled from YouTube...

YouTube has had to pull the plug on its music videos after a dispute with music publishers over the terms of a new music licence. YouTube is locked in a battle with the Performing Rights Society - the rights agency that collects royalties for songwriters, composers and publishers. YouTube claims the licence fee proposed by PRS is prohibitively expensive and would involve the site making a loss on every song played. PRS, on the other hand, says that YouTube is trying to negotiate a fee which is significantly less than it has previously paid despite the massive increase in YouTube viewing. The parties are also arguing over the scope of the licence. Despite the posturing, the parties are optimistic that they will come to an agreement eventually with both saying they hoped that the videos would be available again soon to its users - for YouTube visitors this will be music to their ears...

Motive irrelevant in determining database right infringement says ECJ - Apis-Hristovich v Lakorda, European Court of Justice...

A Bulgarian court referred a number of questions to the European Court of Justice ('ECJ') after Apis had brought proceedings to stop Lakorda from unlawfully extracting and re-utilising substantial parts of Apis's legal information system. Apis claimed that it had made a substantial investment in the compilation, verification, systemisation and updating of databases regarding Bulgarian legislation and case law. The EU's Database Directive protects creators of databases who have made a substantial investment in obtaining, verifying or presenting a database by prohibiting someone from extracting material from it and then using the whole or a substantial part of it. This is known as the 'sui generis' database right. Lakorda - founded by individuals who had previously worked in Apis's software department - denied unlawfully extracting substantial parts of the Apis modules to produce and market their own case law and legislation modules.

The ECJ said that extraction takes place for the purposes of the Database Directive as soon as data was transferred and stored elsewhere, regardless of the motive for transferring the information. Therefore, whether the user of the database intended to use the database in competition with the database right owner was irrelevant (other than for assessing the damage caused to the owner). The ECJ also found that it was immaterial that the transfer of the contents of a protected database to another medium resulted in a different arrangement or organisation of the relevant information. The presence of features in Lakorda's modules which were identical to Apis's - such as editors' notes, references to English translations, commands and fields - could be interpreted as evidence of extraction, said the ECJ, unless that coincidence could be explained by factors other than a transfer between the two databases. The fact that the materials were not accessible to the public could constitute circumstantial evidence of an extraction.

The ECJ also considered the application of the Database Directive to a body of materials which consisted of several different modules. As in this case, it was necessary to determine whether a module itself was protected by the database right and if so to compare the amount of material allegedly extracted or re-utilised from the module with the total contents of that module alone. If the module itself was not protected, but the module was part of a body of materials which was eligible for protection, then the comparison had to be made between the volume of materials allegedly extracted or re-used from that module and other modules against the total body of materials. The ECJ made clear that the database right applied independently of whether the database or its contents were protected by copyright.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

CYBERCRIME/SECURITY

Cybercriminals focus on mass data harvesting operations...

Trojan horse programs that steal data increased by more than 15 times in 2008 compared to 2007, indicating that cybercriminals are now focusing on harvesting data. Scansafe - the security firm - said data theft Trojans made up 14% of all malware blocked by the firm in 2008 compared with 6% in the previous year, with most of the malware being delivered to users through trusted web sites. Commercial and personal data theft continues to provide a lucrative business for cybercriminals. Scansafe warned businesses to be alert to an increase in intellectual property theft and illegal monitoring of all network traffic.

Facebook targeted five times in seven days by malicious hackers...

Facebook was subjected to five separate malicious attacks in a seven day period by hackers trying to steal members' personal data. Social networking sites are a prime target for data thieves who capitalise on the trust and social links upon which those forums are founded. Four of the five attacks were made by the introduction of malicious applications which aim to steal saleable information from the profiles of members who add the application. The fifth attack was a new variant of the Koobface virus which first wormed its way onto the site in December 2008, as reported here: <http://www.upload-it.com/editArticle.aspx?ID=3025>.

The new strain uses a Facebook message to try to get people to visit a fake YouTube page and once there the user is encouraged to install the malware by placing an image from the Facebook user's profile on the video page to make it look more plausible. A senior security adviser at Trend Micro has called for Facebook to review its policy of waiting until members report problems before vetting an application. This suggestion, however, has been rejected by Facebook, which stated: 'Our philosophy is that having an open system anyone can participate in is generally better.'

BBC becomes a cybercriminal for the day...

The BBC played at being a cybercriminal for the day when its technology programme, *Click*, carried out an experiment which involved using a botnet - a network of hijacked computers - to launch a distributed denial of service ('DDoS') attack. A DDoS attack bombards the target web site with requests for access to make it inaccessible. Cybercriminals threaten high-traffic web sites with an attack unless the site operators pay a ransom. Web sites often just pay up to avoid the potential significant disruption to trade. *Click* showed just how easy it was to acquire a relatively cheap botnet and take down a back-up site owned by Prevx, the security company. Apparently, the experiment was with Prevx's consent. The experiment showed that only 60 hijacked machines were required to overload the site's bandwidth. Users are often not aware that their computers are being controlled remotely by cybercriminals. Following the research, the owners of the hijacked computers were told that their computers were infected and they received advice on how to make sure they were protected in future. But whilst the BBC has demonstrated how easy it is for cybercriminals to carry on their 'business' consider yourself warned: don't try this at home - if you try the experiment you may end up contravening the Computer Misuse Act.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

DATA PROTECTION/PRIVACY/CONFIDENTIALITY

USB sticks continue to be lost as organisations fail to learn data security lessons...

Despite the reporting of many high profile data losses over recent years, it appears that UK organisations are still failing to protect portable data devices such as laptops and USB memory sticks. Lothian and Borders police is the latest organisation to admit losing an unencrypted USB stick. The stick contained various information including vehicle registrations. USB sticks increase vulnerability to data loss as their physical size decreases and they become easier to misplace. Credant Technologies has claimed that an estimated 9,000 USB sticks were lost in the last year at UK dry cleaners. Meanwhile, Kroll Ontrack has reported that 90% of laptops sent for data retrieval did not have any form of encryption. A spokesman for Lothian and Borders police has said that the recent data loss did not compromise any individuals involved in police investigations.

ICO to prosecute author of construction workers' blacklist...

The Information Commissioner's Office ('ICO') has confirmed that it will prosecute Ian Kerr, the owner of the firm Consulting Association, which ran a database used by the construction industry as a 'blacklist' for over 15 years. The database, which contained sensitive personal information relating to over 3,000 construction workers - such as their personal relationships, trade union activity and employment history - was seized during a raid by the ICO in February. Evidence also revealed details of the construction firms that had subscribed to the blacklist for an annual fee of £3,000.

The ICO has confirmed its view that Mr Kerr's operation of the blacklist amounted to a serious breach of the Data Protection Act. Mr Kerr stored individuals' personal data without their knowledge or consent and unlawfully traded in that data to allow the construction industry to vet a prospective employee for as little as £2.20 a time. Mr Kerr had not even notified (or 'registered') with the ICO to process data as required by the Act.

The ICO took swift action and served an enforcement notice requiring Mr Kerr to comply within seven days. The ICO said that Mr Kerr since shut up shop and vacated his business premises. The construction firms are not off the hook either - the ICO is still considering what action to take against those found to have used the system.

Government closes 'gateway' to data sharing powers in response to widespread criticism of its proposals...

The government has closed the 'gateway' to data sharing powers - for the time being at least - in response to widespread criticism of the proposals contained in the Coroners and Justice Bill. The Information Commissioner's Office ('ICO') had originally supported the government's plans to introduce greater powers to enable it to permit or require the sharing of information between government departments, agencies and in some cases the private sector. The ICO has since spoken out against the measures contained in the Bill saying that the provisions are too wide and the safeguards are too weak. Some people had also protested against the powers on the basis that they would lead to a 'Big Brother' society. Opponents were concerned that the plans would have allowed information from the public sector to be shared with the private sector without the knowledge or consent of the individual concerned. The government has now decided to conduct a public consultation process on the issue.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

Retention of fingerprints and DNA of persons suspected but not convicted of a crime violates right to privacy, rules ECHR...

The UK's policy of retaining fingerprints and DNA data of persons suspected, but not convicted, of a crime violates their right to privacy under Article 8 of the European Convention on Human Rights. The European Court of Human Rights ('ECHR') made its ruling following an application made on behalf of two former suspects, one of whom was 11 years old, who were arrested and charged but not convicted. Despite the acquittal of one and the discontinuation of the case against the other, the police refused to destroy their fingerprints, DNA samples and DNA profiles. Applications for judicial review of this decision were rejected all the way up to the House of Lords in the UK.

The UK government had argued that the retention of the data was necessary and proportionate in the fight against crime. The ECHR, however, found that the interference with a persons right to privacy in this respect could not be justified as necessary in a democratic society because:

- the UK was the only jurisdiction in Europe which allowed the indefinite retention of fingerprints and DNA material of any person of any age suspected of an offence, whereas other Member States had limited the retention and use of this data to achieve a proper balance of the competing interests;
- the question was whether the extension of the DNA database was proportionate and struck a fair balance between the public and private interests notwithstanding that the information had contributed to detecting and preventing crime. However, the policy of retention was a blanket policy and indiscriminate – it didn't take into consideration the nature or gravity of the original suspected offence or the suspect's age.

The UK government will now have to consider the records included within the existing database very carefully in light of the decision of the ECHR. The ruling is likely to have major implications for the future of the database - in particular, the government may have to remove the records relating to people not actually convicted of an offence.

1 in 4 government databases may be illegal...

11 out of 46 government databases may be illegal under human rights and data protection laws. A report commissioned by the Joseph Rowntree Reform Trust claims the rogue databases should be scrapped or substantially resigned. The report, produced by the Foundation for Information Policy Research, counted and assessed 46 databases in operation or in the process of being built by the government. The report gave only six the 'green light' as being effective, proportionate and necessary with a proper legal basis for any privacy intrusions. Those given the 'red light' - indicating that they are likely to be illegal - included the national DNA database, the national identity register and the NHS detailed care record. The UK's database culture has seen the increased centralisation of data, creating greater risks of data losses affecting millions of people – such as the loss of two CDs in October 2007 by HM Revenue & Customs which led to this report being commissioned. The report recommended that the provision or sharing of personal data be limited to strictly defined purposes only and sensitive data should, in most cases, be confined to local systems rather than national.

Google's launch of Street View in the UK arouses fierce opposition from lobby group Privacy International...

Google's has launched the UK version of Street View to a blaze of fierce opposition from lobby group Privacy International. The organisation has now submitted a formal complaint about the service to the Information Commissioner's Office ('ICO'), asserting that the safeguards promised by Google do not actually give adequate notice or deal with photographed people's data fairly as required by data protection laws. Google's service, which has already been rolled out in the US and some other European countries, allows users to browse pictures taken at street view. The picture view can be rotated a full 360 degrees and users can effectively wander along roads and through the cities at street level. In the UK, it currently applies in 25 cities from Aberdeen to Southampton, and growing.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

Google has always maintained that it has taken significant steps to ensure that it protects the privacy of individuals. It uses technology to blur out faces and licence plates that appear in the images and provides tools for flagging and reporting inappropriate images for removal. Last summer, the ICO had ruled that the measures taken by Google were sufficient to ensure that privacy was maintained. Privacy International, however, is not convinced. It says it has received over 200 reports from members of the public complaining that they are identifiable via the service. Amongst the reports, one woman said she was recognisable outside her new home to which she had moved to escape a violent partner, and two work colleagues described their embarrassment after an image of them in an apparently compromising position was circulated at their workplace.

In its objection sent to the ICO, Privacy International declared that Google's claim that its face blurring system would result in a 'few misses' was a 'gross underestimation'.

Mark Weston, head of the Commercial, IP and IT team at Matthew Arnold & Baldwin LLP, told Sky News recently: 'The technology ratchet has turned another notch. This is yet another new technological tool which although useful raises legal issues. It is important that the individuals' safeguards are put in place to ensure the tool is both trusted and useful.'

Google introduces controversial behavioural advertising system...

March was a busy month for Google. Not only did it launch its contentious Street View service in the UK but it also introduced a behavioural advertising system which will track users' online activity to display relevant adverts to users. Google's new system will be piloted on its YouTube video sharing site and on web sites which use Google's AdSense technology to choose and display advertisements.

Behavioural advertising systems are notoriously controversial. They have been criticised over the lack of information provided to users and their ability to opt out. Google, however, claims that it recognises privacy concerns and is committed to transparency and user choice. Each advert shown by Google will have a label on which a user can click to get more information about how Google chooses adverts to show users and the information it collects to do this. For the system to work, Google will observe users' web surfing and create a list of interests for each individual. In contrast to other behavioural advertising systems, Google says that users will be able to edit the list of interests that it compiles for them. It also claims that users will be able to opt out of the service altogether.

Google is one of the signatories to the good practice principles on online behavioural advertising established by the Internet Advertising Bureau. For more on the good practice principles see the article entitled 'Good Practice Principles for online behavioural advertising unveiled by IAB' in this month's Upload-IT.

Good Practice Principles for online behavioural advertising unveiled by IAB...

The Internet Advertising Bureau ('IAB') and a number of key stakeholders in online behavioural advertising have published a set of Good Practice Principles. The Principles are described as complementing UK data protection legislation and aim to provide Internet users with transparency and greater choice in relation to behavioural advertising. They focus on three core themes - notice, user choice and education. In particular, each signatory (called a 'member') agrees to:

- Provide a clear and unambiguous notice to users that it collects data for online behavioural advertising purposes - including information about the types of data collected, how it will be used and how users can decline advertising from the member.
- Allow consumers easily to decline online behavioural advertising and prominently display information on its web site informing users how to do so.
- Provide the IAB with up-to-date information on users who have declined online behavioural advertising.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

- Inform and educate users about online behavioural advertising, provide the IAB with a web site containing this information and provide a link to the IAB's information portal.

The self-regulatory guidelines, which are supported by the Information Commissioner's Office, will come into effect in September. Signatories to the Principles already include AOL, Google, Microsoft, Phorm and Yahoo!. For more guidance on online behavioural advertising, visit the web site established by the IAB and its members at www.youronlinechoices.co.uk.

Transfer of Madoff data to US would not breach data protection laws rules High Court – In the matter of Bernard L Madoff Investment Securities LLC, High Court...

The High Court has given liquidators of Bernard Madoff's companies permission to transfer to the US personal data relating to one of the UK companies and said this would not breach UK data protection legislation. Madoff's companies were behind a high-profile US\$50 billion fraud. The Data Protection Act 1998 normally prohibits the transfer of personal data outside the European Economic Area unless the country to which it is being exported ensures an adequate level of data protection. The US is not a country which is deemed to have adequate protection and therefore the transfer of the requested data would usually be barred unless an exception applied.

The High Court ruled that one such exception applied here. It was in the public interest for an alleged fraud on this scale and of this complexity to be investigated – thus satisfying the exemption of the transfer being 'necessary for reasons of substantial public interest'. The High Court also said that the exemption relating to a transfer which is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) was relevant in this case. The ruling, however, only related to specified information. The Court refused to issue a blanket permission for any further information which the parties may require to be transferred in the future.

Barclays persuades High Court to continue injunction against the publication of leaked internal documents – Barclays v Guardian, High Court...

Barclays Bank has successfully persuaded the High Court to continue a temporary injunction which is preventing the Guardian newspaper from publishing internal documents belonging to the bank which have been leaked by a Barclays employee. The documents relate to financial transactions that Barclays was proposing to implement between 2005 and 2007 with a view to avoiding UK tax. They contain client information and legal advice as to the tax treatment of the proposed transactions. The Guardian had published the documents in full on its web site for approximately four hours before Barclays obtained an interim injunction which required the Guardian to remove them from its site and prevented it from disclosing them to third parties.

The High Court decided that the injunction should be continued as there was a sufficiently realistic possibility of Barclays establishing that the documents contained confidential information and that they had been disclosed in breach of confidence. It said that material which was generally available on the Internet was likely to lose its confidential character unless there had been very limited and only partial dissemination on an obscure site which was not available generally to the public without some significant searching. The High Court found that, despite the availability of material for a short period on the Guardian's site, Barclays had a sufficiently realistic chance of convincing the trial court that its appearance had not destroyed the confidentiality so as to characterise the material as being freely available.

In considering the newspaper's right to freedom of speech under the Human Rights Act 1998, the High Court ruled that journalists did not have complete freedom to publish in full confidential documents leaked in breach of a fiduciary duty. In this case, the contents of the documents could have been used to inform and express opinions to stimulate public debate without full publication of the documents.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

DATA RETENTION

Regulations requiring retention of Internet data come into force...

Regulations that require public telecommunications services providers in the UK (known as 'CSPs') to retain Internet related data are in force with effect from 6 April. CSPs will be subject to similar data retention obligations as with the Data Retention (EC Directive) Regulations 2007, which were imposed just on telephone companies from October 2007 in relation to fixed and mobile telephone data. Since the 2007 Regulations came into force, telephone companies have been required to retain the data surrounding every phone call made in this country for 12 months. The Data Retention (EC Directive) Regulations 2009 replace the 2007 Regulations and cover both non-Internet and Internet data.

Previously, CSPs could opt to retain Internet-related data under a voluntary Code of Practice which required the data to be held for six months. Under the 2009 Regulations, the retention period has been increased to 12 months from the date of a communication. Information to be stored includes data relating to the source, destination, time, date, duration and type of communication, as well as the users' communication equipment and, in respect of mobile phones, the location. However, as with the 2007 Regulations, the intermediaries will not be required to store any content of the communications. The 2009 Regulations also require the retention of data relating to unsuccessful call attempts that are stored or logged in the UK. This has been of concern to privacy groups. They 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 2009 Regulations do 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. The Home Secretary has discretion (as with the 2007 Regulations) to reimburse any additional expenses incurred by providers in complying with the Regulations, provided that those expenses have been agreed with the Home Secretary in advance.

Government reveals proposals to store Facebook data...

The government's plans to have a massive central database of data about people's use of Internet and other communications may also stretch to data generated by use of Facebook, Bebo, MySpace and other social networking sites, the government has admitted. The Data Retention (EC Directive) Regulations 2009 requires public telecommunications services providers to retain Internet related data but it does not cover social networking sites such as Facebook or MySpace. The government's multi-billion pound project, the Intercept Modernisation Programme, goes beyond the scope of the Directive. It includes plans to retain information about all telephone calls, emails and Internet visits made by every person in the UK on a central database. The information would then be used to assist the government in its fight against terrorism and other crime without needing to ask other communications service providers for access to their data.

The Home Office has denied claims that there are plans for a database containing the content of emails, texts, conversations or activity on social networking sites. Instead, the information to be included on the database is likely to be similar to the information required to be retained by the 2009 Regulations in respect of other Internet related data, for example the source, destination, date and time of a communication.

DOMAIN NAMES

ToysRUs commits to online retailing by bagging Toys.com for US\$5.1m...

ToysRUs, the toy giant, has demonstrated its commitment to online retailing by paying a massive US\$5.1m (£3.6m) for the domain name toys.com – believed to be the biggest payout for a domain name this year. It does not, however, come close to the US\$14m paid for sex.com in 2007. Sedo, a UK domain name seller, has reported that, whilst sales for .co.uk domain names have halved since the recession hit the UK, more small to medium sized businesses are now buying domains.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

ICANN votes to put limitless domain name policy on hold...

The International Corporation for Assigned Names and Numbers ('ICANN') - the body responsible for regulating the Internet's addressing system - has voted unanimously to put on hold its plans to create a limitless supply of Internet domains. This follows responses to ICANN's consultation, which revealed concerns regarding trade mark protection and the need to make expensive domain name registrations to defend brands. Many brand owners already feel under pressure to register their name and variations of it, including common misspellings, every time a new domain is launched. They do this to prevent cybersquatters or typosquatters from gaining control of the names, which could involve them having a costly and disruptive battle to get possession of the name.

Cybersquatters and typosquatters use names similar to famous brands to pretend to be that business or to attract visitors to an advertising web site or even to try to sell them to the brand owner. Defensive registrations often work out cheaper than having to take legal proceedings to obtain a name from a squatter. A number of businesses already maintain large portfolios of domain names at significant cost.

ICANN will now conduct a series of discussions with concerned intellectual property owners relating to the trade mark protection issues in connection with the introduction with any new generic top level domains.

HARDWARE

Recession hits PC sales – analysts predict global slump of 11.9% in 2009...

Analysts have predicted that PC sales in 2009 will slow down to 257 million globally - a downward slide of 11.9% on 2008. If the analysts turn out to be right, this will be the second period of negative growth in the PC industry's history. 2002 saw a fall in sales in the PC market of 3.2% but this was principally from the corporate side of the market. This time, analysts are predicting that both individuals and businesses will buy fewer PCs, instead choosing to hang onto existing PCs for longer to curb general spending. Although other areas of the industry – such as mini-laptops and netbooks – are on the rise, they still only account for 8% of the market, which will not be enough to prop up the PC industry as a whole.

INTERCEPTION OF COMMUNICATIONS

Big brother laws allow lawyers' conversations to be bugged – Re McE, House of Lords...

The House of Lords has ruled that the Regulation of Investigatory Powers Act 2000 ('RIPA') does allow communications between lawyers and their clients to be bugged. This interpretation of the so-called 'Big Brother' laws is inconsistent with the long established right of lawyers to withhold the details of communications with their clients from the police, prosecutors or courts – known as 'legal professional privilege'. Legal professional privilege is designed to ensure that clients provide the full facts of a situation to their solicitor so that they receive full and proper legal advice. Without the right to legal professional privilege some clients may withhold information in the fear that the communications may be used in evidence against them.

A solicitor, Manmohan Sandhu, was charged at Antrim Magistrates' Court with incitement to murder and intending to pervert the course of justice. Recordings taken of conversations between Mr Sandhu and his clients in Antrim police station were produced as evidence against him. Mr Sandhu argued that it was illegal for the police to record his discussions with clients because of the right to legal professional privilege. The House of Lords, however, ruled that RIPA does allow surveillance of privileged communications. It ruled that legal professional privilege cannot be absolute and that it has exceptions. It went on to say that if covert surveillance of legal consultations was not permitted where there were strong grounds to suspect the privilege was being abused the law would give dishonest lawyers an unjustified immunity from prosecution. The House of Lords acknowledged that

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

there may be other situations where it would be lawful to monitor privileged consultations. It used examples of where it is necessary to obtain information of an impending terrorist attack or prevent the threatened killing of a child but did not attempt to define the limits of the possible exceptions.

IT AND INTERNET USE

Failing to upgrade spam filters is costing big businesses thousands of pounds each year...

Failing to upgrade spam filtering systems that offer 99.5% accuracy may be costing big businesses thousands of pounds a year in lost productivity. These are the findings of McAfee's March 2009 spam report. The report revealed that most organisations assume that spam filtering systems with 95% accuracy are good enough but in fact those systems typically miss two spam messages a day, costing one minute of lost productivity per employee. The report estimates that the total annual loss for an organisation with 1,000 employees based on a 252 day working year and an hourly wage of US\$30 an hour would be around US\$126,000 (£90,000).

PUBLIC LAW

New corporate offence of 'negligent failure to prevent bribery' proposed in draft Bribery Bill...

A new corporate offence of 'negligent failure to prevent bribery' by persons working on behalf of a business has been included in the draft Bribery Bill. The Bill will replace the common law offence of bribery and the Prevention of Corruption Acts 1889 to 1916. If passed, it will establish two general criminal offences of bribery - promising or offering a bribe; and requesting, agreeing to receive or accepting a bribe; in each case, at home or abroad. A separate offence of bribery is created for bribery of a foreign public official. The new corporate offence opens the door, though, for businesses to be guilty for actions of their employees. Businesses will need to show that they have good systems in place to prevent bribery if they are to have a chance of avoiding conviction under the new corporate offence.

The Bill would also increase the maximum penalty for bribery from seven to 10 years' imprisonment and an unlimited fine.

TRADE MARKS AND PASSING OFF

L'Oréal brings its battle against eBay to the UK courts...

L'Oréal has brought its ongoing fight against eBay to the UK High Court as part of its bid to protect its brand and distribution network. L'Oréal claims that eBay should be doing more to prevent the sale of counterfeit products on its web site. However, eBay argues that it simply provides the forum for the introduction of buyers and sellers to one another and has defended its anti-counterfeiting procedures, which include a dedicated anti-fraud squad and an annual spend of more than £10m to fight fraud.

Similar cases have been brought by L'Oréal in France, Belgium, Germany and Spain and also by other brand owners in Europe and the US with mixed success. The Belgian courts have already rejected L'Oréal's claims that eBay does not do enough to prevent the sale of counterfeit goods on its platform. Meanwhile, the US courts rejected Tiffany & Co's claims that eBay's anti-counterfeiting actions were inadequate and found that eBay was not responsible for all trade mark infringement on its site. In contrast, Louis Vuitton Moët Hennessy, the luxury goods company, persuaded a French court that there were 'serious faults' in eBay's processes which led to them allow counterfeit sales which damaged the reputation of the luxury brands.

Watch this space for the latest instalment of eBay's battles against the brands...

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

Market trader found guilty of trade mark infringement offence...

A market trader has been found guilty of possessing counterfeit trainers bearing Nike and Bathing Ape names and logos that were likely to be mistaken for registered trade marks with a view to selling them. Wallati Singh was charged by Essex Trading Standards with the criminal offence under Section 92 of the Trade Marks Act 1994. The High Court found that Mr Singh's evidence failed to show that he acted on reasonable grounds in his belief that the goods were genuine and so his defence failed. In particular, Mr Singh had taken the goods to market in a van belonging to his brother who had a caution for selling counterfeit goods, he knew the price of the trainers were low, and he had relied only the word of a drug addict suffering from an overdose to satisfy himself that the trainers were not 'dodgy'. In the view of the High Court, Mr Singh could have hardly done less to establish that the goods were genuine!

The decision of the High Court illustrates just how difficult it is to establish a defence to the offence of possessing goods bearing a sign likely to be mistaken for a registered trade mark with a view to selling or hiring them. Brand owners are likely to welcome the ruling made by the High Court which shows the offence is one of near strict liability.

Court provides clear vision on the right to oppose Community trade mark applications - Alberto Jorge Moreira v OHIM, European Court of First Instance...

The European Court of First Instance ('CFI') has provided some helpful guidance on the interpretation of trade mark opposition provisions under Article 8(4) of the Community Trade Mark Regulation ('CTM Regulation'). Alberto applied for a declaration of invalidity of four figurative European Community trade marks ('CTMs'), owned by General Óptica SA, which incorporated the words 'General Optica' in class 42 for opticians' services. The application was based on Alberto's ownership of the earlier Portuguese business establishment name 'Generalóptica' in relation to optical, precision and photographic apparatus.

Article 8(4) provides that upon opposition by the proprietor of a non-registered trade mark or sign used in the course of trade of more than mere local significance, a Community trade mark ('CTM') will not be registered if rights to that sign were acquired prior to the priority date claimed for the CTM application and the owner of the sign had the right to prohibit use of a subsequent mark, under the law of the EU Member State governing that sign.

The CFI said the rationale of the requirement relating to the sign's significance was to limit the number of conflicts between signs by ensuring that an earlier sign, which is not significantly important, is prevented from challenging the validity of a CTM. The CFI found that the applicant had not established that the name Generalóptica was recognised outside of a certain Portuguese town with 120,000 inhabitants and had not shown that it had developed any advertising activity to promote the business establishment outside of the town. The CFI, therefore, dismissed Moreira's application for a declaration of invalidity of General Óptica SA's CTMs on the basis that Generalóptica had not more than mere local significance.

The CFI suggested a number of ways in which an opponent or an applicant for invalidity could assess whether the sign relied upon satisfied this requirement, such as:

- showing a network of economically active branches;
- through invoices issued outside of the region in which it has its principal place of business;
- by press cuttings showing the public's recognition of the sign;
- by showing that there are references to the business in travel guides.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881

If you would like further information on any of the items in this month's newsletter or anything else Commercial/IP/IT- related, please contact:

Paul Gershlick – Associate
The Corporate Commercial Group
Commercial/IP/IT Team

Matthew Arnold & Baldwin LLP
21 Station Road
Watford
Herts, WD17 1HT
Tel: 01923 208816
paul.gershlick@mablaw.co.uk

The information set out in this Bulletin does not constitute legal advice. No responsibility is assumed for its accuracy and it should not be relied upon. Specific legal advice should be sought on the issues described, if necessary.

London: 85 Fleet Street,
London EC4Y 1AE. **Tel:** 020 79364600
Fax: 020 7842 3300

Watford: 21 Station Road,
Watford, WD17 1HT **Tel:** 01923 202020
Fax: 01923 215050

Milton Keynes: 401 Grafton Gate,
Milton Keynes, MK9 1AQ **Tel:** 01908 687880
Fax: 01908 687881