

UPLOAD-IT - 1 JUNE 2008

CONTRACTS

- ***Court of Appeal rules that repeated substantial delays in payments entitled innocent party to bring contract to an end - Alan Auld Associates v Rick Pollard Associates, Court of Appeal...***

Both parties were chartered engineers. Alan Auld Associates ('AA') had contracted to provide project advice to an authority in relation to the removal of radioactive waste. AA and Rick Pollard Associates ('RP') entered into a verbal agreement pursuant to which RP would provide advisory work at an hourly rate, he would submit monthly invoices, and these would be paid once the authority had paid AA. Despite the authority promptly paying each invoice and numerous complaints from RP, AA substantially delayed payment of 19 invoices. RP then refused to carry out any further work.

AA brought a claim against RP for the losses it had suffered as a result of having to engage another company to provide the advisory work. However, RP counterclaimed for payments owed to him under the agreement on the basis that the agreement had come to an end by acceptance of the fundamental breach of contract, entitling RP to terminate. The trial judge and the Court of Appeal found in favour of RP. The Court of Appeal ruled that AA's substantially persistent and cynical breaches of the agreement against a background of RP's repeated complaints were sufficiently serious to entitle the innocent party to bring the contract to an end.

- ***BERR invites businesses, consumers and enforcers to give their views on consumer law...***

The Department for Business, Enterprise and Regulatory Reform ('BERR') has published a consultation paper to gather views and evidence on whether and how to reform UK consumer law. The consultation comes at a time when the EU is also reviewing eight EU consumer protection Directives. Whilst BERR advocates the current law as being well developed and providing a good level of protection for consumers, it believes the regime is unduly costly and inflexible. BERR is also keen to ensure that the law is able to adapt to new developments in media and technology.

The review will cover the following areas:

- ◆ The scope for simplifying existing law and improving flexibility and future-proofing whilst maintaining protections for consumers.
- ◆ Exploring various ways of simplifying and rationalising enforcement.
- ◆ Investigating the options for improving consumer empowerment and redress.

BERR is particularly interested in what businesses, consumers and enforcers think of the current regulatory framework, including which aspects they find challenging or burdensome and the practical effects the legislation has on them. Other key concerns to be addressed in the consultation are the options for reform, consumer empowerment and redress, and securing compliance with the law.

This consultation comes against the backdrop of a recent OFT report, which revealed that more than one in two consumers had suffered unfair treatment by a business in the past 12 months and that this was costing consumers over £6 billion a year. For more on that story, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2592>. The consultation is important, as the review could

lead to changes in the law which would have an impact on all consumers, businesses and enforcers. However, any scope for changes will be influenced by existing EU laws and also the outcome of the EU review.

Anyone interested in responding to the consultation should email consumerlawreview@berr.gsi.gov.uk by 31 July 2008.

COPYRIGHT AND DATABASE RIGHTS

- ***Illegal file sharing host ordered to pay \$110m for copyright infringement...***

TorrentSpy - a file-sharing site which hosted a collection of links to films and music that had been available for peer-to-peer sharing without the copyright owners' permission - has been ordered to pay \$110m (approximately £56m) in damages to the Motion Picture Association of America for copyright infringement. This comes just weeks after the website shut down. TorrentSpy utilised 'BitTorrent', a legitimate file-sharing technology which allows individual users to send and share large files over the Internet without having to use a centralised server. The judgment is thought to be one of the largest fines handed down for copyright theft. TorrentSpy's parent company and its owners have filed for bankruptcy.

CYBERCRIME/SECURITY

- ***New law passed that makes possession of extreme pornography an offence...***

A new law has been passed that makes it an offence to possess 'extreme pornography'. This would involve images where there is, or appears to be, sexual activity with animals or corpses, or extreme sexual violence that appears to be life threatening or likely to result in serious injury. There would be defences for people who had a legitimate reason to have the image or did not know they had it, or who removed it soon after receiving it as an unsolicited image. Until now, it was already an offence to publish, distribute and possess for gain extreme pornographic material under the Obscene Publications Act 1959, but the Criminal Justice and Immigration Act 2008 goes further and makes mere possession an offence that could lead to imprisonment. At the same time, the new Act also increases the maximum prison term for breach of the Obscene Publications Act and widens the scope of what is covered by the term 'photograph' for the purposes of child pornography laws.

The Act specifically applies to Internet service providers ('ISPs') based in the UK and European Economic Area, but there are exemptions from liability for ISPs that closely follow the Electronic Commerce (EC Directive) Regulations 2002. These are where the ISP acts as mere:

- ◆ Conduits – where an ISP transmits information on behalf of a recipient of a service or provides access to a communications network, provided that it did not initiate the transmission, select the receiver or select or modify the information contained in the transmission and the information is only stored for as long as reasonably necessary for the transmission.
- ◆ Caches – where the ISP simply caches information for the sole purpose of facilitating access to the information for other users of the service, provided the ISP acts 'expeditiously', on obtaining actual knowledge that the information has been removed from the network or access has been disabled

(whether by court order or otherwise), to remove or disable access to the information.

- ◆ Hosts of information – where the ISP hosts information at the request of a recipient of the service, provided the ISP has no actual knowledge of illegal activity and once it does become aware of such activity it acts quickly to remove or disable access to the information.
- ***Law for protection of children to be extended to the possession of non-photographic depictions of child sexual abuse...***

The Government has announced that it will create a new offence for possession of a wide category of non-photographic visual representations of child sexual abuse which will include computer-generated images, cartoons, drawings, sculptures and other representations not already covered by law. If enacted, the new offence would apply only to material that is pornographic – i.e. produced solely or principally for the purposes of sexual arousal - and images must depict the sexual abuse of children and must be of an obscene character. The maximum penalty for possession of the prohibited representations will be three years' imprisonment or an unlimited fine (or both).

People in possession may have defences in line with the existing defences under the Criminal Justice Act 1988. For example, there are likely to be defences for those who need to have contact with material in the course of legitimate work, those who come across the material accidentally and did not know what it contained, or those who receive it on an unsolicited basis and did not keep it for an unreasonable time. Internet service providers, in particular, will need to ensure they are aware of the defences available to them and it is likely they will wish to implement procedures to ensure that the proscribed material is blocked or deleted as soon as they become aware of it so that they can rely on the lack of knowledge defence.

- ***Reports of slow progress made in the battle against software piracy...***

Software piracy rates in the UK have fallen by 1% to 26% in the last year. The figures were revealed in the Business Software Alliance's ('BSA') in its annual report. However, the BSA has stated that there is still an unacceptable amount of UK organisations that flout software licensing regulations and 'there's a huge amount yet to be done'. The BSA represents software licensors and helps them obtain licence fees for illegally copied software. Unlicensed software often arises as a result of businesses neglecting their licensing obligations and how much they should pay for permitted use.

Even more discouraging is the finding that the global rate of piracy actually grew in 2007. It now stands at 38% - an increase of three points on 2006. The BSA has attributed this increase to a growth in the sales of PCs in countries where piracy was widespread. The US contains the lowest piracy rate at 20% and Armenia is now the worst offender – where 93% of all software used is done without the copyright owner's permission.

- ***Blogger fined under Telecommunications Act for posting threatening and offensive message...***

A blogger who ranted on the Internet about his perceived mis-treatment by the police and the Crown Prosecution Service after he was charged with theft offences has been convicted under the Telecommunications Act of posting a message that a reasonable person would find threatening and offensive. He was fined £150 with £364 costs by magistrates in Mold. The blogger's comments had been directed at perceived threats to one of the detectives' new baby. He had originally been

interviewed with theft offences. Those alleged offences have yet to be dealt with, but as a result of his rant the blogger has been charged with more than the original offence.

- ***Businesses fail to take security seriously enough, despite increased spend, as less than 1 in 10 businesses encrypt laptops...***

Less than one in 10 businesses encrypt laptop hard drives and about 3 in 10 protect confidential data from being taken on USB sticks, despite the fact that 79% of businesses claim to believe that they understand the security risks that affect them. UK businesses spend even more on IT security, but security breaches still cost them billions of pounds a year. These are the findings of the 2008 Information Security Breaches Survey of 1,000 businesses led by PricewaterhouseCoopers and the Department for Business, Enterprise & Regulatory Reform.

DATA PROTECTION/PRIVACY/CONFIDENTIALITY

- ***Information Commissioner given new powers for breaches of data protection laws...***

A new law has been passed which increases the sanctions for breaching the Data Protection Act 1998. This follows various high-profile breaches in both public sector and private sector. The Information Commissioner – the UK's data protection regulator – now has more in his armoury. The Criminal Justice and Immigration Act 2008 contains the following new provisions:

- ◆ The power to serve monetary penalties on data controllers who commit serious breaches of the Data Protection Act without first needing to serve an enforcement notice on them. Once this provision is brought into force, this would occur in circumstances where the contravention was serious and likely to cause substantial damage or distress, and the data controller either:
 - deliberately contravened the Act; or
 - knew or should have known there was a risk of contravention, and that it would be likely to cause substantial damage or distress, but failed to take reasonable steps to stop this from happening.
- ◆ The prospect of soon-to-be-introduced laws that could lead to two years in prison for anyone knowingly or recklessly obtaining or disclosing personal data without the data controller's consent.
- ◆ The Act has also introduced a defence for anyone knowingly or recklessly obtaining or disclosing personal data without the data controller's consent: for journalistic, literary or artistic purposes in the reasonable belief that this was in the public interest.

This new law is an indication that failure to protect the security of data about people will be treated far more seriously in the future and could lead to higher and more frequent fines and possible imprisonment.

- ***Court of Appeal breaks paparazzi's spell and rules that JK Rowling's son had a reasonable expectation of privacy when walking down the street – David Murray v Big Pictures, Court of Appeal...***

The Court of Appeal has allowed an appeal against a High Court ruling to strike out the claim made on behalf of author JK Rowling's son, David Murray, following the covert taking and publishing of a photograph of David with his parents in a street when he was 20 months old. The Court of Appeal considered the following questions:

- ◆ Was there a reasonable expectation of privacy (under Article 8 of the Human Rights Act 1998)? This was an objective question taking into account of all the circumstances of the case including:
 - the attributes of the claimant;
 - the nature of the activity in which he was engaged;
 - the place at which it happened;
 - the nature and purpose of the intrusion;
 - whether or not there was any express or implied consent; and
 - the effect on the claimant and the circumstances in which and the purposes for which the information reached the hands of the publishers.
- ◆ If there was a reasonable expectation of privacy then how should the balance be struck as between the claimant's right to privacy and the publisher's right to freedom of expression so they can publish (under Article 10 of the 1998 Act)? This would involve a balancing act.

The High Court had ruled that David had no legitimate expectation of privacy, because he was merely doing a routine activity. However, the Court of Appeal disagreed and said it was at least arguable that David had a reasonable expectation of privacy. The case should therefore proceed to trial in order to decide whether the interference with his privacy was justified in light of the publisher's right to freedom of expression. In reaching its decision in favour of the David, the Court of Appeal considered that the following factors were significant:

- ◆ The fact that David was a child rather than an adult was significant. The action had been brought by David's parents only on behalf of David and not on their own behalf.
- ◆ The child's reasonable expectations about his private life could be ascertained by looking at how his private life had been conducted by those responsible for his welfare and upbringing so that a child courted publicly in order to promote a parent's interest would have less of an expectation of privacy when compared to a child (as in here) whose parents had taken care to keep them out of the public eye.
- ◆ The law should generally protect children from intrusive media attention.

The Court of Appeal further considered that if the trial judge did find that there had been a breach of David's Article 8 right (after balancing it against the publisher's Article 10 right) then it would follow that the processing of David's personal data by publishing or procuring the publishing of the photograph was unlawful under the Data Protection Act 1998 as it would not be 'fair processing'. This opinion of the Court of Appeal - that a breach of one law can result in an automatic breach of the Data Protection Act - confirms the long-held view taken by the Information Commissioner's Office, the UK's data protection regulator.

Samantha Lloyd, assistant editor of Upload-IT, comments: 'This case is significant for those taking and publishing photographs of children as it highlights the particular need to protect a child's right to privacy. Extreme caution should be exercised by photographers and publishers, who should refrain from taking and using photographs of children in cases where the parents of the child have not specifically sought publicity for their child, even where they are involved in apparently innocuous activities such as merely walking down the street.'

- ***Mere taking of a photograph is not enough to interfere with right to privacy – Andrew Wood v Commissioner of Police for the Metropolis, High Court...***

Andrew Wood – the media co-ordinator of the Campaign Against Arms Trade pressure group – had attended an annual general meeting of a public company in which he had bought shares. The police had been concerned that he may have been trying to cause trouble and had taken photographs outside the AGM and sought to obtain his details. Mr Wood applied for judicial review of the police's actions and claimed it had interfered with his right to privacy under Article 8 of the European Convention on Human Rights.

The High Court has dismissed Mr Wood's claim for judicial review and ruled that the mere taking of photographs in a public street was not enough to interfere with a person's right to privacy under Article 8. This case is the first time that the courts have considered Article 8 in the context of photographs taken in public by the State rather than the media taking photographs of celebrities.

- ***University lecturer reprimanded for breaching data protection rules merely for reporting to concerned parent about son's progress...***

Geraint Johnes, a university lecturer at Lancaster University, has been reprimanded by the University's data protection officer after responding to a concerned parent's email giving details of the students courses and workload. Jackie Gardner had emailed Mr Johnes, who is head of economics at Lancaster University, complaining that her son was not fully engaged, that he was receiving only three hours of lectures a week and requesting details of her son's performance. In response, Mr Johnes had explained that Mr Gardner had at least four hours' contact time per week in addition to regular project meetings. This innocuous exchange became the subject of controversy when Mr Gardner complained to the University that it had released the information without his consent. Following the complaint, the University admitted a breach of the data protection rules. Mr Johnes has been warned about his future behaviour and told that any further 'illicit disclosures' would be reported to the HR department.

- ***Large HMRC disciplinary figures for data breaches: is this a comfort or a concern?...***

HM Revenue and Customs ('HMRC') has disciplined more than 600 staff over the last three years for illegitimately accessing people's personal data, according to figures revealed by the Government. In a large number of the cases, the staff had been sacked for inappropriately accessing private data on individuals.

Samantha Lloyd, Upload-IT's assistant editor, comments: 'Whilst the Government has hailed these figures as demonstrating the strength of HMRC's disciplinary procedures, one has to express some concern about the amount of people employed by HMRC who go on to breach HMRC's strict policy of forbidding staff from accessing customer records unless they have a legitimate business need. This comes on the back of various recent data protection scandals, including the loss of 25 million people's records in one incident last year.'

DATA RETENTION

- ***Government tightens its grip on phone and email records...***

Two pieces of news have emerged concerning the increased regulation surrounding data retention. Firstly, the Government has announced that it will be looking to pass the Communications Data Bill. This would involve Internet service providers being subject to similar data retention obligations that were imposed on telephone companies from last October. Since last year's laws came into force, telephone companies have been required to retain for 12 months the data surrounding every phone call made in this country. This is not the contents of the call itself but details of who called whom, when, for how long and from where. Over 100 public authorities have the right to call for the disclosure of that communications data from the telephone companies. When the new Communications Data Bill is introduced, Internet service providers will need to retain details of people's electronic communications, including emails and Voice over Internet Protocol (or calling people over the Internet). People's website habits may also be retained.

Those data retention laws have been brought in as a result of an EU Directive. However, the UK Government has gone further. In the UK, the data can be handed over not just for detection of really serious crimes (such as terrorism) but also for much wider purposes. And now, according to the second piece of news, discovered by *The Times* newspaper, the Government actually proposes to store all of the data itself. Over one trillion emails and 50 billion texts alone (not to mention the number of telephone calls) were sent last year.

Paul Gershlick, editor of Upload-IT, spoke live on BBC Radio about this issue. He comments: 'No one doubts the need to preserve data to try to stop really serious crimes such as terrorism. However, the Government's plans for one super-database begs the following questions: Given the current existing laws, why the need for one database? Given its recent track record with data handling, is the Government the best person to look after that data? How much is this going to cost the tax payer to look after so much data?'

Mark Weston, head of Commercial/IP/IT at Matthew Arnold & Baldwin, was also critical about the further move towards a 'big brother' State when he was interviewed live on Sky News about the issue, and as he wrote recently on the Society for Computers and Law website: 'The Information Commissioner, Richard Thomas, has previously warned that we are 'sleepwalking into a surveillance society'. His office has again reiterated these concerns in light of these most recent proposals.'

DEFAMATION

- ***Offences of blasphemy and blasphemous libel abolished...***

The common law offences of blasphemy and blasphemous libel have been abolished. The abolition was brought in by the recently passed Criminal Justice and Immigration Act 2008. The changes will take effect on 8 July 2008.

DOMAIN NAMES

- ***Appeal panel overturns ruling which had ordered the transfer of the mspace.co.uk domain name to MySpace...***

A Nominet appeal panel has overturned the Nominet arbitration panel's ruling that MySpace had the right to have the domain name mspace.co.uk transferred to it.

Upload-IT reported in February this year how MySpace had succeeded in showing that it had legitimate rights in the domain name and that the registration of that domain by the other party had been in 'bad faith'. For more on this article, please click here: <http://www.upload-it.com/editArticle.aspx?ID=2463>.

The case was controversial as Total Web Solutions ('TWS') – the registrant - had registered the domain name six years before MySpace was founded. However, MySpace argued that TWS had changed the way the site was used to take advantage of the goodwill and rights that the popular social networking site had generated. Despite finding in favour of TWS, the appeal panel expressed scepticism about TWS's activity but concluded that, given the absence of sufficient material to prove that TWS was being untruthful, it must leave it to MySpace to take the matter to the courts, where a full hearing of all the evidence could be tried and tested. In some cases, the quick, cheap and informal dispute resolution service offered by Nominet was not appropriate for complex cases, but that did not stop someone from taking his complaint over someone else's use of a domain name to the court to adjudicate.

E-COMMERCE REGULATIONS

- ***French court rules RSS website liable for having snippets from source websites that invaded privacy...***

A French court has ruled that three websites which published snippets of a story about Sharon Stone, the actress, on their websites through an RSS feed from a third party website was liable under the country's strict privacy laws for that material. 'RSS' stands for 'Really Simple Syndication' and it is a method by which data can be collated from the web and made available to a reader in one place without the reader having to keep scouring all of his or her favourite sites. The owners of the websites – Planete Soft, Aadsoft and Lespipoles – were found liable because the infringing third party articles had been available via their websites. The RSS link was a link to the source website together with a very brief summary of the content. That was too much for the French court. In the UK, there has not as yet been any reported case establishing liability merely for providing a link.

EMPLOYEES

- ***44% of UK businesses report firing employees for violating email policies...***

44% of UK businesses have reported sacking employees in the past year for violating email policies and 78% of UK business reported disciplining workers for this offence. In addition, 53% of UK businesses have been found to regularly audit employees' outbound emails to ensure that they are not breaching email policies and 47% have conducted investigations into email leaks of confidential or sensitive data in the last year. These are the findings of a survey carried out by Forrester on behalf of Proofpoint, an email security firm. The survey also found that whereas monitoring external emails used to be the way to find out what sort of information was leaving the business's systems, the advent of new methods – such as blogs, message boards, social networking sites and web-based email – now posed increased threats.

MISLEADING ADVERTISING

- ***ITV receives record fine of £5,675,000 for abusing premium rate services...***

ITV has been fined by Ofcom - the broadcasting regulator - a total of £5,675,000 for serious breaches of Ofcom's Broadcasting Code in relation to the abuse of premium rate services ('PRS'). The fines for breaches of Ofcom's Broadcasting Code consisted of:

- ◆ £3 million fine on LWT for three competitions within Ant & Dec's Saturday Night Takeaway;
- ◆ £1.2 million fine on LWT for Ant and Dec's Gameshow Marathon;
- ◆ £1.2 million fine on Granada Television for Soapstar Superstar; and
- ◆ £275,000 fine on ITV2 for breaches when repeating programmes.

Other breaches of the Broadcasting Code were found to have occurred on I'm A Celebrity Get Me Out of Here!, People's Court, ITV Playalong, The Mint and Glitterball but no fines were imposed.

The reported breaches included:

- ◆ Selecting finalists before the telephone lines had closed.
- ◆ Staggering the selection of finalists so that viewers did not have an equal chance of winning.
- ◆ Selecting finalists on their basis of suitability to be on screen and because of where they lived.
- ◆ Shortlisting individuals known to the production team as potential winners.
- ◆ Ignoring viewers' votes and choices and finalising results before lines had closed.
- ◆ Failing to inform viewers that interactive competitions had concluded when repeating programmes.
- ◆ Failing to inform viewers that broadcasts were not live and interactivity no longer available when repeating an interactive dating programme so that viewers were charged for wasted calls.

Ofcom's findings also revealed that ITV programme makers had totally disregarded their own published terms and conditions and that the systems for monitoring and reporting on the use of PRS were completely inadequate. However, investigations into allegations made about The X Factor did not reveal any breaches of the Broadcasting Code and a detailed minute-by-minute analysis of the call data for the 2007 final confirmed that Leon Jackson was correctly announced as the winner over Rhydian Roberts.

In reaching its decision on the level of the fines, Ofcom took into account the additional £7.8 million pledged by ITV for viewer compensation and for charity. Ofcom is continuing its investigations into other ITV programmes and a number of programmes on BBC radio and television.

- ***Ryanair's advertising practices come under fire again as ASA refers it to the OFT...***

Ryanair has come under fire again from the Advertising Standards Authority ('ASA'), which has referred the low cost airline to the Office of Fair Trading ('OFT'). The ASA have been investigating various complaints made in respect of Ryanair's advertisements for a period of two years and on seven occasions have found them in breach of the British Code of Advertising, Sales Promotion and Direct Marketing (the 'CAP Code'). However, it was Ryanair's repeated refusal to confirm the number of

flights available in relation to its £10 seat offer advertised in national newspapers in 2007 that led to the ASA referring Ryanair to the OFT.

The ASA found that Ryanair persistently misled customers by advertising misleading prices, making inaccurate and denigratory comparisons with competitors, failing to make clear restrictions excluding customers from offers and failing to provide evidence to claims they were making. One such spat, as reported by Upload last November, can be read here: <http://www.upload-it.com/editArticle.aspx?ID=2317>. Ryanair has hit back at the ASA by issuing a statement saying that it has submitted a formal complaint to the OFT about the ASA's 'unfair procedures, bias and factually untrue rulings' against it.

The ASA administers the CAP Code, which is a code of practice governing the content of adverts and marketing communications. Although the Code does not have legal force, it is best practice to comply with it, as failure to do so can result in bad publicity and ultimately an inability to obtain advertising space. The ASA tends to work as a self-regulatory deterrent and advertisers nearly always comply with rulings. In rare occasions such as this, the ASA may refer the matter to the OFT, which has powers to obtain injunctions from court for breaches of the Control of Misleading Advertisements Regulations 1988 and the Consumer Protection from Unfair Trading Regulations 2008.

TRADE MARKS AND PASSING OFF

- ***US jury rules that two and four stripes breach Adidas's three stripe trade mark ...***

A nine person federal jury in Kansas has found that Collective Brands' two stripe and four stripe shoes breached Adidas's three stripe trade mark and has ordered Collective Brands to pay Adidas \$305 million in damages. This is not the first time Adidas has pursued organisations for infringing its trade mark rights. It has mounted several actions in Europe and the US over its stripes. Many manufacturers and retailers claim that the stripes are not distinctive enough to be trade marked and are merely decorative designs.

Adidas has also received recent support from the European Court of Justice ('ECJ') against H&M – the retailer - following a reference from a Dutch court. Whilst the ECJ acknowledged that stripes as decorative elements must be available to all, this must not restrict the rights of a trade mark holder. The question to be considered, the ECJ had said, was whether consumers would be mistaken as to the origin of the product featuring the same logo and characteristics as the logo except for the fact that they consisted of two rather than three stripes.

- ***Court says establish whether elements of later composite mark have independent distinctive roles when judging possible confusion with earlier registered mark – Rouselon Freres v Horwood HomeWares, High Court ...***

The owner of already registered marks 'PROFESSIONAL SABATIER', 'SABATIER' and 'SABATIER LION' - which had been registered in class 8 on the trade marks register - applied for two later UK composite trade marks 'JUDGE SABATIER' AND 'STELLAR SABATIER' - which had just been registered in classes 8 and 21 - to be invalidated on the basis that there was a likelihood of confusion between them and the earlier marks. The hearing officer at the Trade Marks Registry decided that there was no likelihood of confusion between the marks and so refused the invalidity request.

On appeal, the High Court has ruled that, in this case, the word SABATIER retained an independent distinctive role in the later marks and there was a likelihood of confusion making it appropriate to invalidate the later marks in respect of class 8. The Court said that when considering whether a composite trade mark carried a likelihood of confusion with an earlier mark it was necessary to consider whether the earlier mark had an independent distinctive role within the later mark before answering the questions of whether there was a likelihood of confusion.

UNSOLICITED COMMUNICATIONS

- ***Large but hollow victory for MySpace against junk mailers...***

MySpace – the popular social networking site – has secured a judgment against Sanford Wallace and Walter Rines - two junk mailers - after they had used MySpace accounts which they had created or taken over by stealing passwords, in order to email MySpace members with over 700,000 unsolicited messages. The messages had appeared as if they had come from a trusted friend and they asked the recipients to view a video or visit a website. Those websites then generated money for the pair based on website hits or by trying to sell a product to the MySpace members. MySpace claimed that sending the spam had cost it money and generated hundreds of complaints from its members. Despite MySpace being awarded \$234m (£120m) (US\$300 per unsolicited message) – a total award that is thought to be the largest ever against senders of unsolicited emails - the damages were obtained in default as the men failed to attend court. It may therefore be a hollow victory if MySpace is unable to collect the damages from the offenders.