

UPLOAD-IT - 1 JANUARY 2008

COMPETITION LAW

- ***Alleged cartel participants face possible jail terms after OFT brings first criminal proceedings under Enterprise Act...***

Three businessmen have been unceremoniously arrested at Heathrow Airport on their return to the UK and promptly charged by The Office of Fair Trading for allegedly dishonestly agreeing to fix prices, limit supplies, allocate markets and customers and rig bids contrary to the Enterprise Act 2002. The men will presumably be used to such humiliation now, having originally been arrested in the middle of an industry conference in May 2007 in the US. The OFT - the regulator in charge of enforcing competition law in the UK - has taken action to fine various businesses that have either entered into uncompetitive agreements or abused their dominant positions, but this is the first time that criminal proceedings have been brought against individuals for cartel activity. If found guilty, the men face up to five years in prison and unlimited fines.

The charges result from transatlantic co-operation between the OFT and the US's Department of Justice and follows a plea bargain under which the men agreed to come back to face possible charges in the UK rather than serve sentences that had already been handed out to them in the US. The three men had each agreed to jail terms in the US for around two years and fines of about US\$100,000 as part of the plea bargains. The people involved are Bryan Allison (managing director of Dunlop Oil & Marine Ltd), David Bramner (sales and marketing director of the same company) and Peter Whittle (sole proprietor of PW Consulting (Oil & Marine)). The men will now stand trial in the UK and the men will start with a normal presumption of innocence in the UK trial irrespective of the US plea bargains.

- ***Not much Christmas spirit in town as Danish tree growers accused of fixing prices...***

Danish Christmas tree growers have been charged with ripping off customers by allegedly unlawfully agreeing to rig prices. The Danish competition authorities brought the action against the Danish Christmas Tree Growers' Association after they had sent out price guidelines to its members. This was in spite of warnings from the competition authority not to do so on two previous occasions. The prices of the trees rose by 25% in 2007. The tree growers are accused of having meetings in which they were encouraged not to undercut their competitors.

- ***Microsoft faces new Windows tying claim – this time for its web browser...***

Microsoft is facing fresh allegations in the European Union that it has been abusing its dominant position by tying products to Windows. This time, Opera Software has complained to the European Union that Microsoft unfairly tied Internet Explorer – Microsoft's browser that is used by 80% of the market – to Windows. Opera is a Norwegian browser supplier with 1% of the market. It has asked the European Commission to require Microsoft to provide unbundled versions of its products. There have also been complaints that Microsoft is not following web standards to enable interoperability with its systems. These new allegations come hot on the heels of Microsoft's settlement of a €497m fine by the European Commission from a case that stretches back to 2004. In that first case, Microsoft was fined for unfairly bundling (or tying) its Media Player software into Windows and also for withholding vital information about Windows from makers of server software.

- ***Competition law victims can sue for compensation but not exemplary damages - Devenish v Sanofi-Aventis, High Court...***

In 2001, the European Commission had fined certain vitamin manufacturers about €800 million for contravening EU competition law by participating in a cartel. Following that decision, some businesses that had purchased vitamins from that cartel brought a claim for damages in the High Court. It was not disputed that the claimants could be awarded compensatory damages for losses they could prove they suffered, but – due to the difficulty of quantifying those losses - they also sought exemplary damages to punish the wrongdoers and an account of profits.

The High Court has decided that although exemplary damages may be available in principle, they would not be available in this case as the European Commission had already fined the cartel participants – and so there would be 'double jeopardy' if they were punished again. Making such an award could also nullify the incentives behind the Commission offering leniency from fines if cartel participants comply with competition law investigations. If the courts would have effectively punished the participants again with damages over and above simply compensating the victims, this would effectively be stating that the Commission's fines were insufficient. That was not something the High Court was able to do. The High Court also said that an account of profits would not be available as compensatory damages would be the proper remedy for competition law cases.

CONTRACTS

- ***TUPE can apply to transfers from the UK to outside the EU - Holis Metal Industries v GMB, Employment Appeal Tribunal...***

In some outsourcing and other service contracts, the provisions of the TUPE Regulations apply. Depending on the circumstances, those Regulations may automatically transfer the liability of employees from one entity to the new entity providing the service. One question that had not been answered until now was whether TUPE applied when the part of the business transferred was going over to an entity based outside of the European Union. In this case, the Employment Appeals Tribunal has answered that TUPE can apply in that scenario.

- ***Service supplier can't just fly away from contract because of third party's failure to agree to ancillary agreement - Ryanair v SR Technics, High Court...***

SRT provided aircraft maintenance services to Ryanair at Stansted Airport. SRT asked Ryanair to provide those services at Dublin Airport instead – and Ryanair agreed. Under a side letter, SRT agreed to grant Ryanair a licence to occupy a section of a hangar that SRT was occupying under a 75 year lease. The licence was going to be for a period of 15 years, subject to the consent of Dublin Airport, the landlord. Dublin Airport decided that it was only prepared to allow SRT to grant the licence to Ryanair for two years. Until Dublin Airport's decision SRT had allowed Ryanair to use the hangar on an ad hoc basis, but SRT revoked Ryanair's licence on hearing of Dublin Airport's decision.

The High Court decided that SRT had breached its contractual obligations to Ryanair. SRT had required the maintenance services to be moved to Dublin Airport. The move assumed that Ryanair's aeroplanes would have sufficient hangar space. The parties had intended for SRT to provide hangar space to Ryanair for 15 years but they knew that Dublin Airport could not be compelled to agree to the licence for 15 years. The High Court would not let SRT escape its obligation to provide hangar space to Ryanair

– and therefore fly away from its agreement to provide services – if Dublin Airport agreed to Ryanair having hangar space for a period of less than the 15 years anticipated. The side letter was to be interpreted as requiring SRT to use its best endeavours to get Dublin Airport to agree to 15 years or as long as possible if Dublin Airport did not agree to 15 years and to seek renewal of the licence on the expiry of the shorter licence. SRT had failed to do this and so was in breach of its agreement with Ryanair.

COPYRIGHT AND DATABASE RIGHTS

- ***Publican suffers defeat in legal case for screening Premier League football through Greek broadcaster rather than from BSkyB -***

Murphy v Media Protection Services Ltd, High Court...

Karen Murphy's conviction for showing a football match in a pub without paying BSkyB has been upheld. She was found guilty of dishonestly receiving a programme included in a broadcasting service provided from a place in the UK with intent to avoid paying a charge for receiving the programme, contrary to Section 297 of the Copyright, Designs and Patents Act 1988. She had a satellite dish and decoder to receive broadcasts of Premier League football games from Nova, a Greek television broadcaster, rather than through BSkyB. The Premier League, which owns intellectual property rights relating to broadcasting Premier League football matches, had granted exclusive rights to BSkyB to show the broadcasts in the UK. It had also granted Nova the right to show games in Greece. Media Protection Services, as agent for the Premier League, succeeded with the prosecution against Ms Murphy in the Magistrates' Court and then the Crown Court on appeal.

On a further appeal to the High Court, Ms Murphy has lost again. The High Court ruled that Ms Murphy had the requisite intent to avoid the charge as she knew that BSkyB had the exclusive right in the UK and that it charged for reception of its broadcasts, and Ms Murphy made arrangements for receiving the broadcasts without paying. It was irrelevant to Ms Murphy's case that she did actually pay a charge - as the payment was to a broadcaster whom Ms Murphy knew did not have the UK broadcasting rights.

CYBERCRIME/SECURITY

- ***Criminal prosecutors issue guidance on when they would consider 'ethical hacking' to be legitimate...***

The Police and Justice Act 2006 updated the Computer Misuse Act 1990 by introducing an offence against making, supplying or obtaining articles for use in offences (such as hacking) under the 1990 Act. The new offence prohibited supply of an article believing it to be likely to be used to commit or assist in the commission of an offence under the 1990 Act. Following the introduction of that new offence, various IT groups were up in arms because it could criminalise so-called 'ethical hacking' - where people supply tools that test the effectiveness of security in IT systems. Since those tools could be used not just to test whether further safeguards were needed to tighten security but also for darker purposes by actually hacking, there was concern that people involved with the supply of those tools may be caught by the new offence. At best, it was unclear what was meant by 'believing' the article to be 'likely' to be used to commit an offence. Critics argued that introducing a legal disincentive to be involved with so-called dual use software could actually have an adverse impact on IT security.

The Crown Prosecution Service has now issued some guidance on the factors to be taken into account when considering whether to prosecute under the new offence. It recognises that there is a genuine industry in testing the robustness of security and the key is to ascertain whether the suspect has criminal intent. Prosecutors should consider the following factors:

- Did the business have in place robust acceptable use policies?
- Were users made aware of what was lawful?
- Did users have to sign a declaration stating intention to comply with the law?
- Who did the suspect think would use the tool and in what circumstances?
- What was the primary purpose for developing the article?
- Was the article available on a wide-scale basis and through legitimate channels?
- Was the article widely used for legitimate purposes?

Paul Gershlick, editor of Upload-IT, comments: 'This guidance is just that: guidance. There is no guarantee that it will be followed. Despite that, people involved in the ethical hacking and security industry should follow it closely. In particular, they should have clearly drafted terms and conditions that warn users not to use the tools for unlawful purposes and they should have a contractual process that get users to sign declarations of intent. Failure to follow the guidance are severe as successful prosecutions could result in prison and/or fines.'

- ***TJX settles with finance giants over customer data theft by hackers...***

TJX - the retailer that owns TJ Maxx and TK Maxx - has reached an out-of-court settlement with various banking businesses over a hack attack that saw the theft of details relating to 100 million credit or debit card transactions over a period of several years. TJX had initially said that at least 45 million cards were exposed - although it turned out that the majority of the cards had expired. It is still believed to be the biggest data breach ever. The data had been accessed via TJX's systems in Watford and Massachusetts when someone accessed the decryption tool for the encryption software used by TJX. The value of the settlement remains confidential. TJX claims that none of its UK customers were exposed to fraud.

- ***One in three websites contain downloadable malware...***

Nearly one in three websites now contain downloadable malware. Those are the findings of research from the Sans Institute. The infection rates have doubled within the previous 12 months. Recent reports show that most infected websites are genuine websites that have been attacked and hacked due to poor maintenance of security patches by their operators.

- ***Australia wants to introduce tough new laws requiring ISPs to filter pornography and violence...***

In Australia, the new Labor government has announced plans to introduce tough rules to require Internet service providers to filter out pornography and violence from what is available to surfers at home and in schools. The aim is to protect children from seeing inappropriate material and having access only to family-friendly websites. Anyone wanting access to the sites deemed inappropriate would have to contact their ISP in order to opt-out of the regime.

DATA PROTECTION/PRIVACY/CONFIDENTIALITY

- ***Department of Health and DVLA are latest in series of public bodies to be found to have carelessly dealt with people's data...***

The Department of Health and DVLA have become the latest public bodies to be pulled up for breaching the Data Protection Act 1998. Following recent prominent data protection fiascos - including the records of 25 million people carelessly lost by Revenue & Customs - three more government data loss scandals have hit the headlines:

- The names and addresses of three million learner drivers were lost by the Driver and Vehicle Licensing Agency's Iowan subcontractor. Despite the data loss having taken place in May 2007, it took seven months for this to be brought to light. At least no dates of birth or financial details were on that list, so potential damage may be limited.
- More data was lost in another, unconnected data loss involving drivers. This time, the Driver and Vehicle Agency in Northern Ireland admitted to having lost data of 6,000 drivers when it sent unencrypted disks to the DVLA in Swansea. The data involved lots of details about the cars.
- In the most worrying breach, the Department of Health posted sensitive personal data - including religious beliefs and sexual information - about junior doctors on the Medical Training Application Service website in a way that was accessible to any visitors. The Information Commissioner's Office - the Regulator in charge of enforcing data protection laws in the UK - has called this data breach 'an unacceptable breach of security'. The regulator has required the Department to sign formal undertakings to comply with the Data Protection Act in future, including:
 - Encrypting personal data on the website if it could otherwise cause personal distress.
 - Regular testing to ensure its computer systems are secure.
 - Training staff on compliance with the Act.

- ***Government looks to change data protection law in light of Revenue & Customs data loss...***

Following the recent careless loss of data relating to 25 million people from families claiming child benefit by HM Revenue & Customs, the Government has launched a consultation into how personal data should be treated in the public and private sectors. The Information Commissioner - the regulator in charge of enforcing data protection law in the UK - is one of two people in charge of the consultation. The consultation will consider changes to the Act and will present options for changing the law to the Government. The Information Commissioner has already called for easier rights to audit premises, and tougher sanctions for misuse of data.

People can send their comments to the consultation before 15 February.

Meanwhile, in an attempt to restore confidence in public handling of citizens' data, the Government has given the Information Commissioner the power to make unannounced spot checks on public sector premises to investigate data security. The Government has also announced that it will publish data security breaches by public bodies and steps taken to prevent them. The Information Commissioner has welcomed the move - but is now seeking more funding to pay for its enhanced responsibilities.

- ***Information Commissioner issues good practice note over steps to consider in order to keep personal data secure...***

The Information Commissioner - the regulator in charge of enforcing data protection law in the UK - has issued a good practice note to help businesses consider the steps they should take to protect the security of personal data that they hold. Under the Data Protection Act 1998, one of the requirements on organisations that hold data about any living individuals is to have appropriate security to protect personal data against unlawful or unauthorised use or disclosure, and accidental loss, destruction and damage. The note gives detailed guidance that includes suggestions for the following areas:

- Considering the types of data and the effects of a security breach.
- Internal lines of authority for taking responsibility for looking after the data.
- Various organisational security measures, such as risk assessments, security policies, checks on staff adherence to those policies and whether external access is provided to data.
- Various employment security measures, including checking out new staff, employment contract measures and staff training processes.
- Physical security measures, including locks, fencing, doors, alarms, limiting potential access by outsiders and shredding policies.
- Computer security issues, including levels of technology used, whether computers are networked, passwords, ringfencing access to limited staff, data back-up procedures and portable devices.

- ***Leeds Building Society loses bank and salary details of staff...***

As if to prove that the private sector is also capable of matching recent large-scale public sector data security breaches, the Leeds Building Society has told its 1,000 employees that it has mislaid their personal data. The lost data includes the staff's bank and salary details. It told staff that there had been no evidence that the lost data had been removed from its premises. The data was lost when the human resources department moved locations. The UK's seventh largest building society has asked its staff to be vigilant, while promising to compensate them if they suffer loss. There is no evidence that any customer details have been lost.

- ***Privacy became even more threatened in 2007...***

Personal privacy came under increasing threat in 2007, according to a report by Privacy International and the Electronic Privacy Information Center. The report detailed global trends in privacy protection and surveillance. It said that a move towards greater surveillance had left fundamental rights to a private life 'fragile and exposed'. It named England and Wales as two territories out of nine where surveillance had become 'endemic'. Others included China and Russia. Greater scrutiny came in two guises: one was government concern over national security concerns; the other was a developing industry over data gathering and analysis.

- ***Sienna Miller scores victory for protecting image rights by claiming damages against The Sun and News of the World for photos taken while she had been filming...***

The Sun and *The News of the World* newspapers have agreed to pay damages plus costs to Sienna Miller after publishing nude photos of the actress taken while she was filming *Hippie Hippie Shake*. News Group Newspapers, which owns the two newspapers, has agreed not to publish the photos. The Xposure Photo Agency has also agreed to pay damages. Miller is still seeking to sue the individual photographer.

DEFAMATION

- ***Reynolds privilege defence not open to newspaper that did not seek claimant's comments or carry out other proper investigations – Malik v Newpost Ltd, High Court...***

Shahid Malik – a Labour MP – brought a libel claim for two publications in a newspaper relating to a local council election in Mr Malik's constituency in which one of the contributors to the publication had lost to a labour candidate. Mr Malik argued the articles suggested that he had been involved in a gang to threaten and intimidate voters and that he was a dangerous extremist. Mr Malik understandably took offence to those allegations. The newspaper had failed to contact Mr Malik before the allegations were published.

The High Court decided that the newspaper did not have available to it the Reynolds privilege defence. That defence was developed in the Reynolds v Times Newspapers case and seeks to protect responsible investigative journalism where the story is in the public interest, even where the subject matter reported was not true. The defence contains certain safeguards so that people cannot just print what they like. In this case, there was no doubt that the subject matter was in the public interest. However, it was not in the public interest to publish allegations without regard for whether they were true or false. The Reynolds defence required that the newspaper must first take steps – such as taking determined steps to obtain a response from Mr Malik or carrying out corroborative checks – neither of which the newspaper had done in this case. Therefore, the conditions of having the Reynolds defence were not made out.

The High Court also made an interesting comment concerning the person who had made the allegations about Mr Malik, as reported in the newspaper. There may well be circumstances in which the Reynolds privilege defence may protect a contributor and not just the newspaper conducting the investigative journalism – but those circumstances did not apply in this case. The election loser had not merely reported allegations but had presented them as fact. The onus was on him to prove that what he said was true.

EMPLOYEES

- ***Recent surveys show businesses see social networking sites as growing problem...***

77% of businesses that allow access to social networking websites such as Facebook and MySpace intend to monitor or limit staff's access to them, according to a survey by *Computer Weekly*. Businesses are more worried about employees losing productivity on those sites (50%) than security (17%) or damage to reputation (3%). Employees with access spent an average of one hour a day on social networking sites. One IT manager surveyed claimed that his company had sacked an employee who had spent six hours a day acting as a moderator on one social networking site.

Meanwhile, another survey – this time commissioned by Clearswift, the content security firm – found that half of the firms surveyed had encountered problems involving employees wasting time on the Internet. Some of those occasions resulted in disciplinary action. Two-thirds of the firms subject to Clearswift's survey blocked access to social networking sites. 43% of the firms surveyed also had to discipline employees for accessing online pornography at work.

Paul Gershlick, editor of Upload-IT, comments: 'All employers need to have proper IT and Internet usage policies. Otherwise, they may struggle to stop employees who expose employers to legal risk or simply waste time from acting inappropriately.'

IT AND INTERNET USE

- ***Milton Keynes becomes first place in UK to have commercial wireless Wimax broadband service...***

Milton Keynes has become the first place in the UK to have commercial wireless broadband service after ConnectMK provided residents and businesses with access to Wimax in December. ConnectMK - a private company formed by MK Council - joined forces with Pipex and Intel Capital to provide the service. More than 1,000 people in MK have already registered to join the Wimax network. ConnectMK aims to make MK the first Wimax-powered wireless Internet city. Wimax is a telecommunications technology aimed at providing fast wireless data over several kilometres. Moira Myers, who heads up the MK office of MAB (the law firm behind Upload-IT) says: 'This is a very exciting project for MK. It shows that MK is the place to be - right at the forefront of implementing pioneering 21st century technologies.'

- ***End of an era as Netscape Navigator is discontinued...***

It is the end of an era as Netscape Navigator is no longer going to be supported from 1 February. It is an incredible turnaround for the one-time near monopolist in the Internet browser market. In the mid-1990s, Netscape had a market share of more than 90% of the entire Internet population. By the time of its announcement, its market share had slipped to less than 1%. The browser lost out to Microsoft's Internet Explorer, which itself also had a market share of above 90% in recent years – although this has since slipped to a still healthy 80%. Along the way, Microsoft had been accused of using anti-competitive behaviour by bundling Internet Explorer with its Windows operating system – a complaint that the European Commission is currently investigating (as reported in this month's Upload-IT). Most of the staff who had worked at Netscape are now developing the Firefox browser. It may be a case of the Firefox Phoenix rising from the flames as its market share is 16% and rising.

- ***Amazon music download service takes another leap forward with signing up of Warner Music...***

Amazon, the popular e-tailer, has received a boost in its effort to set up a music store in competition with Apple's iTunes, with the news that Warner Music is making its music available through Amazon. Warner Music had previously refused to do so because of concerns over the ability of users easily to copy the music from download onto CD format and also to share it with other Internet users. Amazon, which launched its US downloads store in September 2007, has already agreed deals with Universal and EMI. Of the major record labels, it is just SonyBMG that remains to sign up. Unlike iTunes, Amazon's music download stores do not contain digital rights management to prevent copying. That had previously been a stumbling block for Warner Music.

- ***Ask offers alternative to increasing personal data footprint left on Facebook and Google sites...***

Ask is providing a search service that flies in the face of the recent trend by popular websites to collate and retain people's data. The search engine has launched a feature called AskEraser that enables users immediately to delete all records of their searches stored on Ask's servers. This can be contrasted with other recent stories

that raise concerns over the length of time data relating to users is stored and what is done with it.

Google has come under fire for storing details of people's searches for 18 months on its servers. Privacy activists have been concerned that Google was using that data to send people targeted advertising. AOL was also on the receiving end of bad press in 2006, when search data involving 650,000 of its users was released by AOL to help with academic research. More recently, Facebook – the social networking phenomenon – had to change Beacon, its new advertising system, after 50,000 users had complained about it. Beacon tracks web shopping habits on partner sites outside of Facebook and imports that data into Facebook to provide targeted advertising to users; following the complaints, Facebook changed Beacon from an opt-out system to opt-in.

Ask appears to be trying to play to people's fears by raising its market share from less than 5% of the US search market - compared with Google's 60% market share. However, whether it succeeds or not is open to doubt. According to TechCrunch – the technology blog – many consumers appear willing to pay for the best free products with their privacy and take an 'out of sight, out of mind' approach to web use.

MISLEADING ADVERTISING

- ***Ofcom Consumer Panel calls for tough new action on accurate broadband speeds...***

The Ofcom Consumer Panel has called for action to avoid the practice of misleading advertised broadband speeds. Its concern is that broadband speeds advertised as being 'up to' certain levels often come nowhere near those speeds in reality. A recent survey by *Computeractive* magazine found that more than three in five of people who used its speed testing software had access to the Internet at less than half of the advertised speed. The Ofcom Consumer Panel has called for:

- The Advertising Standards Authority to require advertisers of broadband speeds to explain why they can vary.
- Ofcom to establish and administer a mandatory code of practice for Internet service providers in which there would be an agreed process to give consumers best information during and after the sales process. This would involve consumers being told the theoretical maximum speed, what affects the line speed, and the actual speed consumers are receiving two weeks after installation. If speeds are significantly lower than those advertised, the consumer should be able to switch to a different package free of charge or cancel his deal.

MISLEADING SELLING

- ***Channel 4 fined £1.5m for Richard & Judy and Deal or No Deal phone-in competition breaches...***

Ofcom - the media regulator - has fined Channel 4 £1.5m for the unfair phone-in competitions on the Richard & Judy and Deal or No Deal flagship shows. On both programmes, viewers who telephoned in at a certain time had less chance of winning or no chance of winning at all. Eckoh UK, which ran the You Say, We Pay competition on the Richard & Judy show for Channel 4, has already been fined £150,000. Eckoh staff had submitted shortlists for the competition 20 minutes before the closing time for people taking part in the competition. As well as paying

the fine, Channel 4 has pledged to refund to viewers all money that it had wrongfully received, and pay any unclaimed amounts to Great Ormond Street Hospital. Ofcom said the fines would have been higher had Channel 4 not behaved in such a contrite fashion.

This decision follows on from a similar one a few months ago in which GMTV had been fined £2m for having a competition where winners had been selected up to three hours before the competition had officially closed.

TELECOMS

- ***Vodafone fails to break up T-Mobile/iPhone deal in Germany...***

Vodafone has failed to stop T-Mobile, its mobile phone rival, from having exclusive rights to sell Apple's latest must-have device – the iPhone – in Germany. Apple has agreed similar exclusive tie-ups in different jurisdictions – such as with O2 in the UK and AT&T in the US. Vodafone had initially managed to obtain an injunction that required T-Mobile to supply versions of the iPhone that were not tied to a particular network, but that injunction was overturned two weeks later. In the two weeks that the injunction lasted, T-Mobile sold the handset without a network contract for €999 – as opposed to just €399 for an iPhone that also came with a two-year T-Mobile deal. T-Mobile has agreed to unlock the phones at the end of the two-year deals. Although Apple has tried to tie consumers to a single network provider, programs have been circulated that enable users to unlock their iPhones so they can be used on any network. This led to the recent controversy when a software update released by Apple rendered any iPhone that had been unlocked permanently disabled.

- ***Canadian man receives monthly mobile phone bill for over £40,000...***

A Canadian man was shocked to receive a mobile phone bill for the dollar equivalent of over £40,000. Piotr Staniaszek was under the misapprehension that he could use his new mobile phone as a modem for his computer under his \$10 unlimited mobile browser package from Bell Mobility. He did not realise that he would be charged massive extra costs for downloading large files such as high-definition films. Bell has slashed its fee for Mr Staniaszek's use to about £1,500. However, Mr Staniaszek has threatened to fight the charges. He expressed shock that the phone company had not bothered to call him and warn him when the phone charges were escalating so suddenly.

TRADE MARKS AND PASSING OFF

- ***Lacoste says 'ahhh' as small dental practice sees off Lacoste's legal challenge to register its crocodile trade mark...***

Dr Simon Moore and Dr Tim Rumney have won a prolonged legal challenge by Lacoste over whether they could register a crocodile as a trade mark for their small Cheltenham dental practice. They had used a crocodile logo at their practice since 1990 and decided to try to register it as a trade mark in 2004. Since then Lacoste has fought 'tooth and nail' to try to stop the dentist from registering. Lacoste argued that patients would wrongly associate the dentists with being associated with the clothing company. The dentists showed the Intellectual Property Office through a succession of appeals that Lacoste's claims were laughable. The dentists had chosen the crocodile because the reptile had a lot of teeth, and they said the logo looked nothing like Lacoste's. If Lacoste would have won, the clothing giant would have in effect been given a virtual monopoly over the rights to use a crocodile in respect of

any business. For the dentists, the experience has been like pulling teeth, but at least they have won after their prolonged painful treatment through the legal process.

- ***Tarzan cry calls in novel way of registering sounds as trade mark files...***

November's edition of Upload-IT reported that Edgar Rice Burroughs Incorporated, the owner of rights in Tarzan - the jungle hero – had failed to register the Tarzan jungle call as a European Community Trade Mark (CTM) on the grounds that its representation was not capable of being represented graphically. The Tarzan application had included two graphic illustrations of the sound – one of the sound wave representing the sound and the other a spectrogram of the frequencies of the call. This had been rejected by the Office of the Harmonisation in the Internal Market (OHIM), the body in charge of accepting or rejecting CTM applications. Musical notation of sounds have traditionally been acceptable to be sufficient to count as a graphic representation.

Now, though, the Tarzan owner has tried another tack that appears to have had more success. Edgar Rice Burroughs applied to register the sound as a sound track. OHIM has accepted that sound track in principle. The trade mark application is now within a three month period in which third parties may oppose its registration. If successful, the Tarzan cry would be one of the first to go through under new rules introduced by OHIM in 2006 in which it is possible to consider applications for sound mark registrations supported by electronic sound files rather than representations of the sound as a musical note or other annotation that allows someone to recreate the sound.

- ***Use of term in part of computer not seen by average consumers would not constitute trade mark infringement – RxWorks Ltd v Dr Paul Hunter (t/a Connect Computers), High Court...***

Dr Hunter owned the registered trade mark 'VET.LOCAL' including in respect of software and hardware. RxWorks had created a computer system in which that term appeared on computer screens, for example when searching for a particular file. Dr Hunter sent an email to RxWorks and another one to RxWorks' customer complaining about RxWorks' use of the trade marked terms. RxWorks issued proceedings against Dr Hunter for unjustified threats of trade mark infringement.

The High Court has granted RxWorks' claim for summary judgment. Dr Hunter did not have an arguable case that RxWorks' use of the term had infringed his trade marks and the threat of proceedings was therefore unjustified. The Court went through the four-point test for infringement of an identical trade mark, as set out in the recent European Court of Justice case of Céline Sàrl v Céline SA (which can be found here: <http://www.upload-it.com/editArticle.aspx?ID=2254>) and concluded:

- Use of the trade mark was 'in the course of trade'. This was not a high threshold to show. It was not even necessary for the trade mark to be visible at a point of sale – it would suffice if the mark was only available later (such as after a book or CD was opened).
- RxWorks had used the mark without Dr Hunter's consent.
- The mark had been used in relation to goods or services.
- However, Dr Hunter failed on the fourth part of the test. Its use by RxWorks did not affect and was not liable to affect the functions of the trade mark. The meaning of the mark to the average consumer was the critical test. None of the uses of 'vet.local' were ever intended to refer to the software product, the domain or the folders and would not do so to the average consumer. It was merely an

internal name for an aspect of a complex computer system and was hidden away within the workings of the system. It was only likely to be encountered to a significant effect by systems administrators.

Accordingly, there was no trade mark infringement. Since Dr Hunter had not carefully worded his emails regarding RxWorks' use of the name, instead of being the one taking the action he was on the receiving end of a claim for unjustified threats of trade mark action. This could involve damages and costs being paid by him instead of by the person who had used his trade mark. The exact award of damages was left to be decided at a further hearing if the parties were unable to settle the matter out-of-court.

Paul Gershlick, editor of Upload-IT, comments: 'When you have a trade mark and see someone else using it, the temptation is to fire warning shots off. However, if this is not done in the right way, the trade mark owner may end up having an injunction against them and having to pay damages to the person using the name. This case highlights the importance of getting specialist professional advice when someone believes that their trade marks are being infringed.'