INTELLECTUAL PROPERTY AND TECHNOLOGY NEWS
Perspectives • Analysis • Visionary Ideas

COMBATING COUNTERFEITING IN THE UAE

CATCHING UP WITH DATA PROTECTION DEVELOPMENTS IN FRANCE AND TURKEY

ADWORDS IN EUROPE: THE MISTS CLEAR FOR BRAND OWNERS

PERFORMANCE BONDS BALANCING THE SWORD OF DAMOCLES IN MIDDLE EAST IT&T CONTRACTS

FOOD AND BEVERAGE OPERATORS SHOULD IMPLEMENT INNOVATIVE TECHNOLOGIES

LONDON 2012 A SPONSOR’S EYE VIEW
Welcome

I am delighted to welcome you to this second edition of the Intellectual Property and Technology News for the EMEA region. This newsletter joins two sister publications for Asia-Pacific and the US in which we report on relevant developments for clients operating in these regions in the fields of IP, sourcing, technology, commercial and distribution, data protection, media, sport and entertainment.

The bundling of the information in this newsletter is truly reflective of the increased complexity around many of the key issues businesses face today in both their home and their new and emerging markets. It is a very dynamic world in which we operate, conditioned in part by the current macro-economic background but also by the unprecedented investment growth in the creation, exploitation and defence of intangible assets – whether they be new ideas, technologies, brands, designs, know-how or even business models.

So, within the constraints of any such publication, my ambition for our newsletter is to share some of DLA Piper’s thoughts, observations and advice on these issues as a way to demonstrate that as lawyers we are, collectively, able to respond to the most important issues on your mind, and challenges. Our IPT Team across the globe also hope to show you the benefits of local knowledge derived from being physically located in many of the places where you do business. It is also interesting to note that many of the issues that businesses face around the world are increasingly convergent and in keeping with that, many of the articles in this issue are co-authored by lawyers based in a number of countries.

This newsletter is therefore just the tip of the iceberg, and so my open invitation to you is to continue the conversation with us by contacting one of the authors directly.

À bientôt.

Stéphane Lemarchand

Editor’s Column

As the dust begins to settle here in London following what felt like an unexpectedly successful Olympic games (for everyone except the ambush marketers, it seems – see Patrick Mitchell’s piece on page 11), life returns to normal. On the branding side, Google Adwords continue to keep European trade mark judges in gainful employment (see page 9), but there is cause for optimism; not only is the law around Adwords becoming slowly but surely clearer, but there is also news from the UAE of significant steps being made in the fight against counterfeits (see Katie Withers’ piece on page 5). Progress is also being made in Turkey towards a more modern data protection regime; whether developments in France aimed at clarifying how French data protection law applies to a cloud environment will also be a cause for celebration remains to be seen (see our data protection article on page 6). This edition of the Intellectual Property and Technology News from EMEA also includes an update on the challenging market for IT suppliers in the Middle East (Paul Allen, page 10), and a news update from around the region.

John Wilks
Partner, London
John.wilks@dlapiper.com
INTELLECTUAL PROPERTY WEBSERIES

DLA Piper’s international IP team recently held a 45 minute webinar on preparing for the Unitary Patent and Unified Patent Court system, a system which is expected to radically change the way that businesses inside and outside of Europe can protect their inventions and commercialise and enforce their patents.

While political and legal debate continues on the final details, DLA Piper’s panel explained what businesses should be aware of and offered practical guidance on what can be done now to prepare for the new regime.

Chaired by Claire Bennett from our London office, the panel consisted of DLA Piper partners from three of the key European markets: Germany (Julia Schönbohm), the UK (Adam Cooke) and Italy (Gualtiero Dragotti).

A recording of the webinar can be accessed here: www.dlapiper.com/proposed-unitary-patent-webinar

The webinar was the first in a series offering practical guidance from an international perspective on important IP issues that may impact on your business. The next two webinars in the series will be:

Dealing with anti-counterfeiting – a practical guide – 5 December 2012

Protecting your data and databases – February 2013

To register for any of the webinars, please contact natalie.harrison@dlapiper.com.
TELECOMS

HUNGARY, SEPTEMBER 2012

MOBILE NETWORK OPERATORS CHALLENGE THE REGULATOR

The Budapest Metropolitan Court of Hungary annulled the decision of the National Media and Infocommunications Authority closing the auction for the rights of use of frequency related to the provision of mobile telecommunications service in the 900 MHz band.

The final decision of the Authority, closing the auction, was delivered on 9 March 2012. In its decision the Authority designated a consortium of postal services operator, Magyar Posta Zrt., a subsidiary of Hungary’s development Bank, MFB Invest Zrt. and a power utility, Magyar Villamos Művek Zrt., as the winner of the biggest frequency block at auction. As a result of the auction, beside Vodafone Magyarország Zrt., Magyar Telekom Nyrt. and Telenor Magyarország Zrt. (the so-called incumbent operators) a new, fourth mobile network operator (MPVI Mobil Zrt.) entered the Hungarian market.

The incumbent operators challenged the decision of the Authority in court, disputing the participation right of the new mobile network operator in the auction process and the obligation imposed on the incumbent operators to provide internal roaming services to the new market entrant, MPVI Mobil Zrt.

On 17 September 2012, the Metropolitan Court delivered its judgment on the basis of the petitions of the incumbent operators, in which it annulled the entire decision of the Authority. As a result of this judgment, the incumbent operators also lost the frequency blocks they had won in the same auction. This is likely to be especially problematic for the operators who had already started to use these frequency blocks to improve the services they provided to customers.

The decision of the Metropolitan Court is final and non-appealable. However, a special judicial review may be requested from the Hungarian Supreme Court, recently renamed Curia.

TECHNOLOGY

GERMANY – 2012

MUNICH COURT RULES ON SMARTPHONE PATENT DISPUTE

In a continuation of the spate of litigation between the world’s leading smartphone producers, Apple has obtained a court order in Munich to ban all Motorola smartphones that infringe its “Overscroll Bounce” patent, which concerns the technology used to create the appearance that items on screen are suspended from an elastic band when scrolled too far.

It is Motorola’s use of the Google Android OS in its smartphones that has infringed Apple’s rights and hence Motorola is on the hook – the fact that Google owns Motorola is merely incidental. The order entitles Apple, subject to its posting a bond of €25 million, to obtain a permanent injunction across all of Germany covering any infringing Motorola products. For a further €10 million, Apple may enforce the recall or destruction of all infringing products. Motorola are challenging the validity of the patent in question in the European Patent Office.

BRUSSELS – JULY 2012

SECOND HAND SOFTWARE

The CJEU’s judgment in Oracle v. UsedSoft (July 2012) has caused controversy in the software industry. The CJEU ruled on 3 July that copyright holders in respect of software do not have the right to control the distribution of the original copy of that software once it has been “sold” or “ownership has been transferred.” The CJEU ruled that it was irrelevant that most customers received their software by download rather than by physical media, and also ruled that the resale restriction in the licence is not enforceable. However, the CJEU upheld a number of restrictions on the resale of such computer program licences, including maintaining the copyright holder’s right to have exclusive reproduction rights over its creation, and thus anyone wishing to resell their original copy to a third party is required to make it unusable on their own computer when they do so. This judgment moves European law on the resale of software licences in the opposite direction from the US following the Vernor v Autodesk case there.
Addressing illicit trade requires, first and foremost, a legal framework that is adequate to protect intellectual property rights. The UAE is a signatory to the World Trade Organisation Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). Consequently, the UAE’s federal Trademarks Law provides brand owners with the opportunity to register trademarks for specified goods and services, and affords special protection to well-known marks. It is essential that rights holders register their brands as trademarks in order to strengthen their position when tackling importation or re-exporting of counterfeits.

Another key requirement in tackling counterfeits is an effective enforcement regime. UAE Customs officials are now empowered to exercise enforcement procedures at borders. Specifically, the GCC Unified Customs Law permits them to investigate any consignment to ensure it confirms with the declaration, and to seize goods that infringe a UAE trademark. There are differences in the enforcement of border measures between each of the seven emirates of which the UAE is comprised. For example, Dubai, Abu Dhabi and Sharjah have each established specialist IP rights divisions within their customs departments.

Brand owners may also pursue a criminal complaint and/or bring a civil action against counterfeiters. In Dubai, the police have established a special department to deal with trade in illicit goods, and the threat of a criminal prosecution (and imprisonment of up to three years) may be a more effective deterrent than a fine. A specialist division has also been tasked with tackling online infringers, and the courts may order that a website is blocked from access by UAE Internet users until the court has made its decision on liability in a related infringement case.

A civil action can also be brought against an infringer, and a claim may be joined to a criminal complaint. This enables rights holders to be officially represented in the criminal proceedings. Further, economic development departments in the various emirates, who are responsible for consumer protection matters, have a complaints systems in place to deal with shops suspected of selling fakes. For example, the Dubai Economic Development Department (DED) may impose fines and confiscate or destroy counterfeit goods.

Despite variations in enforcement practice across the emirates, the UAE is taking significant steps to combat and deter counterfeit trade. The increasing number of successful raids suggests that the steps taken are bearing fruit for brand owners. For example, in August 2012, the DED seized counterfeit electronics worth Dh 4 million (US$ 1.1 million), including 5,300 televisions and 7,000 DVD players. Earlier in 2012, about 150,000 fake tools were confiscated from warehouses in Ajman and Ras Al Khaimah. In 2011, Dubai Customs estimated that the number of counterfeit goods it seized that year had dropped by approximately 30 percent. During the same period, the number of brands registered with Dubai Customs increased from 182 to 400.

Businesses concerned about counterfeiting in the UAE should ensure that their key brands are registered as trademarks here. The appropriate enforcement method will depend on the target. A significant enforcement action may be necessary to cut off a main supply or manufacturing source, but smaller resellers may require more proportionate enforcement steps. At the very least, brand owners should ensure that consignments are monitored for counterfeit goods by recording details of their trademarks with the relevant UAE Customs authorities.
CATCHING UP WITH DATA PROTECTION DEVELOPMENTS IN FRANCE AND TURKEY

By Carole Uhmoefer, Jonathan Rofé and Burak Ozdagstanıf

The current speed of technological evolution renders it difficult for legislators to keep data protection laws and regulations current and relevant. It is important that data protection law be kept up to date, so as to facilitate compliance and minimise the burden on businesses and regulators.

In France, the data protection authority has published its recommendations for companies planning to purchase cloud computing services. In Turkey, the legislator has accelerated the adoption of data protection legislation, expected to be comparable with that of other modern countries.

FRENCH DATA PROTECTION AUTHORITY ISSUES RECOMMENDATIONS ON CLOUD COMPUTING

Following a request for comments launched in the fall of 2011, on June 25, 2012 the French data protection authority (CNIL) issued recommendations for companies intending to procure cloud computing services. These recommendations preceded by only a few days the publication of the Article 29 Working Party’s final opinion on the cloud, published on July 1, 2012, which is largely in line with the CNIL’s recommendations.

The CNIL considers that cloud arrangements give rise to uncertainties, such as the difficulty of localizing cloud data, and ambiguities concerning the parties’ respective responsibilities and obligations. From the CNIL’s perspective, such uncertainties originate mainly from the standardisation of cloud offerings and the opacity of the technical and operational measures set up by providers.

When publishing these much-awaited guidelines, the CNIL made it clear that among its objectives are to change market (and in particular service providers’) practices.

It is too early to assess the market’s reaction to the CNIL’s recommendations, and the Working Party’s opinion. While neither document is binding, it will be interesting to observe the market’s reaction, as well as any application of the recommendations and opinion by the courts, and of course the negotiations on the revision of the EU Directive, all of which will shape the cloud’s future.

The main points covered in CNIL’s recommendations are:

1. **Identify Data and Processing Operations**

   It is important for cloud customers to identify the data, processes and services they intend to send to the cloud. For each type of processing, the nature of the data (personal data, sensitive data, strategic data etc.) should be assessed in order to take into account any specific requirements (e.g. in France, health data may only be hosted by licensed providers).

2. **Define Security Requirements**

   Despite the standardised business model of cloud computing, the CNIL considers that the customer should define its own security requirements, from the
legal, practical and technical perspective, and analyse whether the services offered match these requirements. Reversibility and availability of the data will be of particular relevance.

3. Conduct a Risk Analysis

The CNIL considers it “essential” that cloud customers conduct risk analyses in order to identify the security measures to be taken. The authority considers that cloud computing raises the following risks in particular, which can, in CNIL’s opinion, be managed principally through contractual provisions:

- loss of governance with respect to processing;
- technological dependency vis-à-vis the provider;
- failure to keep data of different customers separated;
- failure in the chain of subcontractors;
- lack of availability of cloud services;
- non-compliance with legal requirements.

4. Identify the Appropriate Cloud Services

Several offers exist on the market: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Each may be deployed through a public, private or hybrid cloud. Customers should carefully consider the different options available. This may necessitate contracting with different providers depending on the processing, thereby increasing the level of protection as all data are not entrusted to a single cloud provider.

5. Choose a Cloud Provider Offering the Right Guarantees

The customer should choose a provider guaranteeing appropriate security and confidentiality. It is typically the case that in a client-cloud provider relationship, the client acts as the “data controller”, whereas the provider acts as the “data processor”. Nevertheless, with respect to certain types of cloud offers that are standardised (such as public PaaS or SaaS) and for which the customer has limited room for negotiation, the customer is, in fact, not in a position to give any instructions to the provider or even to verify the effectiveness of the security and confidentiality measures. In these cases, the provider could be considered “joint” controller with its customer. In such a “joint” controller situation, the CNIL advises that the contract should clearly define the allocation of responsibility between the parties.

The CNIL has furthermore listed the major points to be addressed in a cloud computing contract, including in particular: compliance with EU principles, rules governing subcontracting, data retention duration, and obligations to cooperate with data protection authority(ies).

6. Reviewing Internal Security Policies

Customers should migrate to the cloud only after having conducted a complete review of their internal procedures. A specific focus should be made on employee authentication, in particular with respect to use of portable devices.

7. Monitor Evolutions

The CNIL recommends regularly performing an analysis of cloud services, taking into account the ongoing evolution of the cloud environment, risks, solutions available on the market, legislation, etc. An additional risk assessment should also be conducted each time the services are subject to a major change, so that the data controller can adapt such measures or solutions as are necessary.

Finally, it should be noted that the CNIL also proposes more than two dozen different forms of clauses that may be included in a cloud services contract.

TURKEY: UPCOMING DATA PROTECTION LAW

Under Turkish law, there is currently no specific legislation on data protection, and as a result data protection in Turkey is currently subject to the general provisions of a number of different laws and regulations. However, that is all set to change as a new data protection law is being progressed through the Turkish Parliament.

Turkey is a member state of the Universal Declaration of Human Rights, and has been a signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data since 1981. However, as there is no specific data protection law yet in force, Turkey has not ratified the Convention yet.

Although there is no specific legislation, Turkey has been taking important steps on this issue towards introducing a modern law related to data protection, which would allow
for potential future harmonisation with equivalent legislation in other parts of the world. In an amendment made in 2010 to the Constitution of the Turkish Republic, a provision was added stating that everyone has the right to protect his/her personal information, and such a right shall include accessing and requesting correction and deletion of such information. The rights enshrined in the Constitution are echoed in the Turkish Civil Law, Turkish Criminal Law and other specific laws, which impose civil, criminal and administrative sanctions for acts violating these rights.

As required by the Constitution, a Draft Law on Data Protection has been pending in the agenda of the Turkish Parliament for a long time. In the last few weeks, the law-making process has been accelerated, and it is expected that the Law will be enacted before the end of the year. The Draft Law is intended to act as a catalyst for change in the way in which data is processed and managed. Its aim is to govern and regulate the protection of personal data, and preserve the fundamental right of privacy. In general terms it permits personal data to be collected to meet legal obligations, if the collection of data is necessary and in the public interest, or if consent is provided.

Being a G-20 country that has a booming Internet economy and rapidly increasing use of technology, cloud computing offerings are being introduced to the market more and more in Turkey. In that context, service providers and customers should follow the developments in this law-making process, and adapt their strategies starting from today, so as to ensure compliance with the upcoming legal requirements.

**TECHNOLOGY AND SOURCING WEBINARS**

DLA Piper’s Global Technology and Sourcing Team are running a series of 45-minute webinars presented by a multi-jurisdictional team providing insights in negotiation and management strategies for complex projects. The webinars are provided free of charge and the training is delivered to your desk without the need for travel.

Charges master class – Click on the link to listen: www.dlapiper.com/charges-masterclass-webinar

Managed service outsourcing of telecoms networks – 28 November 16:30 – 17:15 GMT

To register for any of the webinars, please contact natalie.harrison@dlapiper.com

**THE WORLD’S DATA PROTECTION LAWS:**

NEW DLA PIPER HANDBOOK

The first edition of *Data Protection Laws of the World*, DLA Piper’s 2011/2012 handbook, is now available.

The handbook offers a high-level snapshot of national data protection laws as they currently stand in 58 jurisdictions across the world. It provides a quick overview of data protection law often of great practical significance to businesses. International data transfer restrictions, security obligations and breach notification requirements are among the topics covered.

The handbook also features a section on enforcement – always an important consideration in assessing regulatory risk in any jurisdiction.

Google’s keyword advertising product AdWords is unquestionably the most successful Internet advertising model ever. Google’s revenue from Adwords amounted to US $38 billion for 2011, and is expected to exceed that for 2012. The Adwords phenomenon has led to extensive litigation around the globe, but particularly in Europe, where the Court of Justice of the EU (CJEU) has delivered no fewer than seven judgments in this area since March 2010. While litigation continues around Europe and some uncertainties remain, a recent Spanish decision illustrates that European law on this area is now somewhat clearer, and that brand owners may have an effective remedy to prevent misuse of their trade marks as Adwords.

While AdWords have become a sophisticated advertising tool, the idea behind them is simple: in summary, advertisers choose one or more keywords, and when a user types said keyword into Google’s search bar, the advertiser’s ad is displayed above or alongside the search results.

The Google France cases in 2010 (C-236/08 to C-238/08) set out the guiding principles. First, the CJEU found that Google would generally not be liable. This shifts the focus to the advertiser. The CJEU found that a brand owner could stop an advertiser using the brand owner’s trademark as an Adword, provided the ad does not enable an average Internet user (or enables such user only with difficulty), to ascertain whether the goods or services referred to in the ad originate from the brand owner (or an economically linked business), as opposed to from a third party.

This same reasoning has since been followed and applied to cases involving second-hand goods (Portakabin, C-558/08), Internet marketplaces (L’Oreal v eBay, C-324/09) and brand owners who licence their trade marks to commercial networks (Interflora, C-323/09). Throughout, the key determining issue was whether an average Internet user is likely to be misled as to the source of the goods or services in question. The brand owner’s position was somewhat improved and further clarified by the most recent CJEU decision in the Wintersteiger case, in April 2012. This determined that an aggrieved brand owner has jurisdiction to sue to prevent use of its trade mark as an Adword both in the country where the trade mark is registered, and in the country where the advertiser is based.

Also in April 2012, the Madrid Mercantile Court upheld a claim by Spanish footwear retailer Masaltos.com for an injunction to prevent a competitor’s using the Masaltos’ trademarks as an Adword. This is the first Spanish decision to apply the CJEU’s case-law on Adwords, and as such will give some comfort to brand owners wanting to prevent misuse of their brands as Adwords in Spain.

So, while some issues around Adwords remain unclear (and it will be interesting to see how the English courts apply the CJEU’s rulings in the Interflora and L’Oreal v eBay cases), this area of trade mark law is steadily crystallising, making life somewhat easier for brand owners. But in any event, trade mark owners would be well advised to take positive action to ensure they keep on top of this issue: monitoring use of their trade marks as Adwords understanding and using Google’s Adwords and trade mark policies, reserving their own trade marks as Adwords, and having a policy for tackling infringers are likely to form part of this.
In the Middle East, organisations looking to procure IT&T goods and services will often mandate that suppliers provide a performance bond (PB) as a condition of contract award. Understandably, suppliers may be nervous about this requirement, especially if coupled with all of the usual commercial and legal leverage tools commonly found in IT&T contracts. Some might argue that PBs are a step too far, acting as a “sword of Damocles” which instils fear in a supplier rather than strong delivery focus. Such arguments aside, PBs are a fact of life in the Middle East, meaning that IT&T customers and suppliers alike must negotiate their terms in order to close deals.

A PB is a financial instrument issued by a bank in favour of a beneficiary (i.e., the customer), under which the bank promises to pay monies to the beneficiary in certain circumstances and up to a certain amount. PBs are common in both public and private procurement settings. In public procurement settings, applicable procurement laws may make it impossible to circumvent PB requirements. In either setting, suppliers should not feel that they must blindly accept the requirement, because they may be able to either offer an alternative approach or at least negotiate the terms on which the PB is issued. In this regard, there are numerous elements of the PB and the supporting language of the related contract which can be discussed between the parties in an effort to arrive at a position which is mutually acceptable.

Typically, customers (and banks) prefer the PB to be unconditional/on-demand, meaning that the customer need only call on the bond for the bank to then be obliged to make that payment. As an alternative, pre-conditions can be attached to the PB such that, unless those pre-conditions are fulfilled, the bank will have no obligation to make payment. Such pre-conditions might be as simple as a notice having been sent to the supplier, right through to a court order for damages having been issued against the supplier. The merits and practicalities of including pre-conditions need to be considered by the parties at the time of negotiation.

Although it is not essential, it is not uncommon for the related IT&T contract to include PB-related provisions, including the:

- value of the PB. Typically a PB will be no less than 5 percent of the total contract value, but can be much higher. Customers should be aware that the cost to the supplier of the PB will increase with its value and that such costs will more than likely be passed on to the customer. Accordingly, coming back to the sword of Damocles image, increasing the size of the sword does not necessarily benefit the customer once the sword is already large enough to destroy the deal for the supplier if it is swung;

- duration of the PB, commonly tied to such things as milestones, the term of the contract or a period after the contract ends to cover potential post-completion claims; and

- contractual conditions to be satisfied before the customer may call on the PB. If such contractual conditions are included but not satisfied, a bank that has issued an on-demand bond will still be obliged to make payment once it is called upon (i.e., the PB operates independently of the contract). Inclusion of conditions does, however, have relevance if the supplier wishes to restrain payment under the bond.

Irrespective of what is negotiated, circumstances may arise in which the customer wishes to call on the PB. When a PB is called upon (or when the threat of doing so is great), a supplier may seek an attachment order (effectively an injunction) against the bank in order to delay payment until a substantive case regarding any underlying dispute can be heard. Any unmet conditions contained in the contract may support the relevant court application. If such conditions are not met and payment is made or threatened under the bond, the supplier may also bring or threaten a damages claim against the customer for breach of contract. Given these possibilities, both the customer and the supplier should be aware of the local laws relevant in such proceedings and ensure that their contract management practices will support any such proceedings.

Calling on a performance bond is likely to have grave consequences for any customer/supplier relationship, making it a remedy which is often considered to be one of last resort. If the PB sword is swung, the terms of the PB and the related contract may determine whether the sword lands where it is meant to or misses the mark completely.
A SUCCESSFUL GAMES

The Olympic and Paralympic Games were a fantastic success, both in terms of sporting achievement and sheer spectacle. But what about in terms of legal issues?

This article focuses on one of the issues that filled a lot of column inches in advance of the Games, sponsor protection from ambush marketing.

THE UNIQUE POSITION OF THE OLYMPIC SPONSOR

It’s worth mentioning the unique position of the Olympic sponsor.

With most sports sponsorships, one of the primary reasons (if not the primary reason) for the sponsor entering into the arrangement is to get exposure. It can activate its rights in a variety of ways, but the best way is television coverage – the main and most obvious way being in-stadium branding – on boards and screens around a stadium.

It’s another way of buying advertising time, and establishing a real connection with the sponsored property – accessing a shop window to the world.

Obviously the position of an Olympic sponsor is very different. All Olympic venues are clean, with no sponsor branding, and so this shop window is not there – the shop is closed at the time when billions of people are watching.
Yet Olympic sponsors continue to pay the highest premiums. What they are buying are the “out of event” promotional rights – the right to be associated with the Games, especially the right to use the various logos in marketing activities. Subject to entering into separate arrangements with the individual athletes, Olympic sponsors are also the only people in whose marketing materials athletes competing in the Games can appear during the period of the Games. Each competing athlete is bound by participation arrangements which confirm that they will not otherwise allow their person, name, picture or sports performances to be used for advertising purposes during the Olympic Games.

This “out of event” promotion is where the value lies in Olympic sponsorship, and as such that value has to be preserved by ensuring that it is not available to others.

So, just as Olympic sponsors are in a unique position, what is required to protect sponsorship revenue is a uniquely robust brand protection framework.

**THE LONDON 2012 APPROACH**

The 2012 Games have been viewed by some as providing the highest level of protection yet for those official sponsors and other members of the Games family. Much has been written about the creation of the new statutory London Olympic Association Right, restricting advertising and street-trading in various zones in and around event venues and the ticketing conditions which included lists of restricted items such as “objects bearing trademarks or other kinds of promotional signs or messages (such as hats, T-shirts, bags, etc) which [the organiser] believes are for promotional purposes”.

These protections, controlled by the London Organising Committee for the Olympic Games (LOCOG) and other elements of the organisational hierarchy, were put in place to preserve the exclusivity and primacy of those official associations.

In truth, LOCOG was seeking greater protections than those which were achieved and finally made it onto the statute books. The passage of the relevant legislation through Parliament saw various provisions watered down, following suggestions that the approach being sought was simply too draconian.

However, in spite of this, and in spite of the existence of various potential loopholes (designed to enable businesses to continue as much as possible with their normal operations but which could have been exploited by cunning marketers), the fact is that that the Games were relatively “ambush-free”.

In large part, this was due to LOCOG and the IOC’s meticulous planning and execution of those plans:

**The building blocks**

First, once the legislation was in place, LOCOG produced a comprehensive document explaining the various legislation. Inevitably, this set out their view of the world, taking what might be described as a more conservative view of what remains permissible within the legislative framework than perhaps a court would adopt. However, such was the detail and usability of the document that it became the go-to guide for this area.
Education and enforcement

Second, from a very early time, LOCOG took a very pro-active approach to ensuring that its view of the world, and what is and is not permitted, as set out in this document, was propagated and adhered to.

Alongside this was a commitment to protecting the brand and enforcing the legislative and contractual protections that were at its disposal. Thousands of man-hours were spent here; by way of example, it was reported that LOCOG’s brand protection lawyers accompanied the Olympic torch on every step of its relay around the country, and trading standards officials were highly visible at venues.

There were of course a few instances in which LOCOG did not have things all its own way. For example, a Paddy Power advertisement announced that it was the “official sponsor of the largest athletics event in London this year” but went on to say that the event in question was actually an egg-and-spoon race in London, Burgundy, France. After initially seeking a removal of the advert, LOCOG stepped away. This ability to exercise judgment and so avoid a fight, where (a) chances are you are going to lose, and/or (b) the fight itself will generate more publicity than the “offending” advertisement, is critical.

Practical steps

Third, the IOC learned from the issues that have arisen in previous world events. The ticketing terms and conditions that were put in place (referred to above) are not particularly unusual, and it is fair to say that as with previous events these were not enforced to the letter. However, the IOC’s host broadcaster, Olympic Broadcasting Services, did not transmit any close-ups of groups of men in lederhosen, or women in short orange dresses – lessons had been learnt from previous events, and the organisers were alive to the ambush-marketing traps that had been fallen into previously.

INTERESTING ISSUES FOR THE FUTURE

As mentioned above, Olympic venues are, unusually for sport, intended to be brand-free, clean, environments. However, this is never totally achieved. For example, in London 2012 there were small motorised Minis collecting the javelins in the Olympic Stadium. Also, so long as the rewards are rich and the sanctions limited or non-existent, there will always be the occasional flouting of participation rules by athletes who wear or display branding of one of their own sponsors, or some other person, who is not an official Games sponsor.

None of this is new. The more interesting issue is the athletes’ brands themselves. Surely it cannot be long until the “Mobot”, the “Lightning Bolt” and the “Beast” brands are commercialised in their own right. It’s interesting to think that a sponsor, contributing millions of dollars to an event, cannot receive any exposure at that event, but, by simply turning up, the athletes are accessing priceless marketing opportunities for their own personal brands – the eyes of the world are on them and the shop is open for business.
**FOOD AND BEVERAGE OPERATORS SHOULD IMPLEMENT INNOVATIVE TECHNOLOGIES TO DRIVE SALES AND REDUCE COSTS**

By Hinal Patel

Unlike other participants in the leisure industry, F&B operators have lagged behind in their use of technology to augment and enhance the customer experience. Although there is some movement in this now, we cannot but think that F&B operators are missing a trick with the slow pace at which they are embracing new customer-facing technologies.

This article looks at why F&B operators might want to quicken the pace at which they implement innovative customer-facing technology solutions, which, we submit, could drive increases in revenue and reduction in costs.

**DIFFERENTIATION**

Using technology to enhance, or even as a central part of, the customer experience has the benefit of differentiating an F&B operator’s brand from its competitors. We are seeing Pizza Express successfully deploy this strategy in some of its restaurants and even Gordon Ramsay at Claridge’s has its wine list on iPads. Used in a way that compliments the F&B operator’s brand and customer experience that F&B operator is seeking to achieve, use of technology ‘front of house’ can be fun, impart greater information regarding the brand, menu items, offers and even the surrounding location, and ultimately help to keep the F&B operator’s brand at the forefront of customers’ minds.

**IMPROVE CUSTOMER TURNOVER TIME**

We have seen a number of brands use technology to speed up the time between when orders are taken to the bar or kitchen being notified. However, this process could be streamlined even further if the customers placed the orders themselves – certain F&B operators have already deployed solutions that enable this. Customers can also settle their bills themselves, for example, through their mobile telephone, thus speeding up the payment transaction process. All of these time efficiency gains can be achieved in a way that enhances the customer experience, and importantly, does not impact the consumption time the customer has so it is not as though the customer is being hurried.

**CRM AND LOYALTY**

With greater use of technology with customers, there is the opportunity to gather information on customer preferences such as around mealtimes, food and drink, level of spend, and so on. This data can be analysed to ensure that the F&B operator’s marketing efforts are targeted to appeal to different types of customers, drive customer loyalty and ultimately a higher spend per customer.

**LOWER OPERATIONAL COSTS**

Along with the advantages described above, F&B operators should see a decline in operational costs. For example, if customers can order and pay for their food and drink themselves, in the right outlet or location, the F&B operator could increase the numbers of customers per waiting staff as such waiting staff can attend to more customers. Additionally, with electronic menus, the cost to update menus should drop as F&B operators will no longer incur printing and/or binding costs. Another example of how costs could be saved is if payments are made through mobile or other electronic means, cash-flow will improve (potentially improving debt repayment costs) and banking and security-related costs could diminish.

F&B operators should see new technologies as an opportunity to improve financial returns through enhancing customer engagement, experience and loyalty, as well as increasing efficiency across the operation. In such a tough economic climate, this has to be a no brainer.
As we come out of the recession, the technology sector has emerged as a beacon for hope, a sector where real growth is possible. There remain challenges, however, which may lead to changes in business models and practices. We intend to look at these shifting landscapes and the changing legal framework which surrounds them.

Join us for a legal update and discussion session on current opportunities, challenges and risks for the technology sector.

Hear from our experienced lawyers and industry panels and have your chance to ask questions and share experiences with others in the sector.

This seminar is FREE and aimed at managers and legal counsel in the technology sector.

ABOUT DLA PIPER
We are a global law firm with over 4,200 lawyers worldwide spread across 77 offices and 31 countries. Our reach is global, but our focus is local. From our offices across the Americas, Asia Pacific, Europe and the Middle East, our legal and business advisers provide a comprehensive range of services to local, regional and international businesses.

HOW CAN WE HELP?
DLA Piper is a full-service business legal provider with a focus on the technology sector. We have lawyers around the world who are experienced at working with technology companies throughout the development cycle. Our experience in the technology sector is wide ranging: from advice on market-leading IT procurements, to financing technology companies to advising on major disputes between suppliers and consumers as well as taking action to protect intellectual property rights.

WHO DO WE WORK WITH?
Our clients range from multinational, Global 100 and FTSE 100 companies to emerging enterprises. We advise a number of West Coast US companies on their EMEA-wide legal needs. Our view is that legal advice should be pragmatic and solution driven as well as technically excellent and we work closely with our clients to build strong, long-standing relationships.

PROGRAMME AVAILABLE HERE:

To book a place at this seminar, please contact:
Jessica Peacock on 0113 369 2643 or email jessica.peacock@dlapiper.com
ALL-IN
DLA PIPER’S
GAMBLING RESOURCE

All-In is an online resource focused on the fast-moving global gambling market. DLA Piper’s global gambling team have created a dedicated site to deliver topical legal and regulatory updates from professionals throughout our network. Our content is designed to provide updates on pure gambling regulatory and legal matters (i.e. changes in legislation, most recent case law, enforcement attitudes) together with IP and IT issues that we feel affect stakeholders in the sector. Our global presence not only facilitates the speed in which we can report on developments but also provides invaluable local knowledge and insight.

Visit All-In at blog.dlapiper.com/gambling