September 2009

Review

Commercial

Welcome to the first issue of a new quarterly commercial review brought to you by the Hammonds' Commercial Team.

We hope that you will find this Review interesting. It provides a brief and informal insight (is that possible from lawyers?!) into some of the most recent commercial developments.

We are not aiming to tell you everything that you need to know about each development, just to alert you to current topics and so if any particular article is of interest to you and you would like any more information, please contact either Vicky Wilkes, Stuart James or Sally Jones, who will be happy to help.

Over the coming months we are trying to develop the Review into something you find useful and informative, but without too much legal jargon. Any comments or feedback you may have are welcome. Again, please direct any comments you may have to Vicky, Stuart or Sally.

Vicky Wilkes
T: 0121 222 3518

Stuart James
T: 0121 222 3645

Sally Jones
T: 0121 222 3444

Online advertising

Online behavioural advertising (or "OBA" to jargon junkies) is becoming increasingly important to businesses that advertise on line. In simple terms, OBA is the practice of sending targeted online advertisement to an Internet user based on their online habits and browser history.

The PR disaster triggered by advertisement network operator Phorm, recently highlighted OBA technologies and the legal basis of their use. Phorm caused controversy when it developed its own OBA technology, "Webwise", which operated by partnering with Internet service providers to monitor users' complete web behaviour (also referred to as "deep packet inspection"). This was then trialled without the users' knowledge. This raises not only data protection issues but also issues around the EU e-privacy rules and the unlawful interception of online communications.

Whilst the UK's regulatory authorities had previously given the green light to OBA technology, complaints from users and lobby groups have led the European Commission to investigate the use of OBA technologies in the UK. The investigation is ongoing but any businesses using OBA technology should consider adopting the Internet Advertising Bureau's self-regulatory guidelines, which propose best practice steps for businesses that collect user data and monitor users' browsing habits for advertising purposes.

The guidelines are available online at www.youronlinechoices.co.uk.

Combatting rogue traders?

It has been just over a year since the Consumer Protection from Unfair Trading Regulations 2008 came into force. The Regulations were introduced to prevent unfair, misleading and aggressive practices and detailed a blacklist of 31 practices that may be deemed unfair. The blacklist includes persistent and unwanted solicitations and falsely stating that a product will be available for a limited time.

Only enforcement authorities such as the Office of Fair Trading can enforce the Regulations by bringing civil and criminal actions, and officers or managers of businesses could find themselves personally liable for a fine or even a prison sentence of up to two years if convicted.

Although the main effect of the legislation to date has been to crack down on unscrupulous small enterprises, including dodgy handymen in Wiltshire and unlawful pyramid selling schemes in Bristol, particularly in the home maintenance and improvement sectors, the approach of Tiscali in their case against BT (*Tiscali UK Limited v British Telecommunications plc*) has shown a novel and creative use of the legislation which other businesses should take heed of if Tiscali succeed.

In Tiscali's case, Tiscali did not argue that it had a claim under the Regulations (as individuals and companies cannot bring claims under the Regulations) but it did argue that, by breaching the Regulations, BT had engaged in interference with Tiscali's business by unlawful means. In an interim judgment, the High Court gave Tiscali permission to bring a case on this basis.

Hammonds

Dear learned friend

One of my major customers has just gone bust and still owes me for a large order. It looks as though I will not recover my money and I am worried this may happen with other customers. Are there any signs I can watch out for?
Mr Everworried

Dear Mr Everworried,
It is always wise to try and shut the stable door before the horse bolts and indeed there are ways in which you can tell if the door is slowly opening… but enough of the analogies. If you have any concern about a particular customer being able to pay you there are a number of signs that may prompt you to take action sooner rather than later. These signs can include:

1. Has the customer started to take longer to pay, is only making partial payments only or paying erratically? This may indicate a fall in available cash. Look out for lump sum payments "on account" of outstanding invoices as this is a potential indication that the customer is marshalling its cash.

2. A customer in a declining financial position may attempt to create creditor pressure by raising disputes about invoices and performance levels. Look to see if the customer corresponds in a more formal way than it has before (e.g. written correspondence rather then telephone calls) or is seeking to create an evidential paper trail alleging breach of contract.

3. Has the financial director recently resigned? Although the director cannot escape the risk of personal liability for wrongful trading by resigning, he may feel that resigning is his only option if, in his opinion, the figures that he presents to the board do not justify the customer's continued trading.

4. Is there any news that other suppliers have stopped supplying the customer or is the customer's identity or reputation suffering (either because it is directly sullied or because it suffers by comparison with competitors)?

Acting early may greatly reduce the effects that a customer's financial difficulties can have on your business.

Yours sincerely,
Learned Friend

Never signed, doesn't bind?

A couple of recent court decisions should send out warning signals to parties negotiating contracts as it now appears that the conduct of the parties whilst the contract remains unsigned may have unexpected consequences...

In a recent case, the High Court held that even though the contract itself was not signed, an email exchange whereby a seller of shares confirmed to the purchaser's agent that he was willing to proceed on and accept the terms of a draft contract was enough to bind the parties to its terms (*Grant v Bragg*).

However, in a recent Court of Appeal case, the parties continued to provide and pay for services even though the letter of intent they had signed had expired. The Court held that a clause in the as yet unsigned contract, which said that the contract did not become effective until parties had executed and exchanged counterparts, prevented the contract from coming into existence until this condition was fulfilled. *(RTS Flexible Systems v Molkerei Alois Müller GmbH*).

These cases are a reminder that parties should ensure that their conduct reflects their intentions. Letters of intent should generally be used (and extended where necessary) which include relevant binding obligations as required before the contract is agreed and signed. If a party does not intend to be bound, it should ensure that its conduct reflects this, for example, by conducting negotiations on a 'subject to contract' basis or expressly declaring that their conduct is not binding.

A privacy notice…what's that?

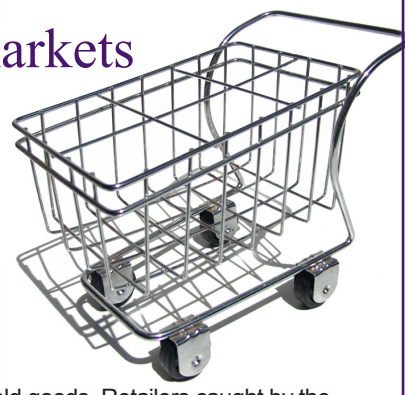
Consumer research has revealed that 50% of consumers still do not understand the privacy and marketing notices contained in many of the online and paper forms they are often asked to sign. This revelation has led the Information Commissioner's Office (ICO) to launch a new "Privacy Notices Code of Practice", (the Code) which is aimed at helping organisations provide more user-friendly privacy and marketing notices.

The Code encourages organisations to get away from using legalistic language in their privacy notices and ensure that they are "clear" and "genuinely informative" so that the people it is aimed at are able to understand it. The Code emphasises the need for privacy notices to enable individuals not just to understand how their personal information is to be used but also what the consequences of this are for them.

Whilst compliance with the Code is not mandatory the ICO has expressly stated that it will take compliance with the Code into account when it receives a complaint that information has been collected in an unreasonable way.

The Code provides some practical examples of both good and bad privacy notices and a copy of the Code is available at www.ico.gov.uk.

Getting tougher with supermarkets



In early August, the Competition Commission (CC) announced that it has adopted the new Groceries Supply Code of Practice (the Code). The Code replaces the much maligned Supermarkets Code of Practice and this comes after the CC's inquiry into the alleged use by some supermarkets of their buying power to transfer excessive risks and unexpected costs to their suppliers.

The Code applies to retailers who have a turnover of over £1billion attributable to the retail supply of "groceries" which includes food and drink, cleaning products, toiletries and household goods. Retailers caught by the Code will include amongst
others ASDA, Marks & Spencer, WM Morrison, Sainsbury's, Somerfield, Tesco and Waitrose.

The Code contains a fundamental requirement that an overarching fair dealing provision must be included in every contract between retailers who are subject to the Code and their suppliers. The Code also covers a number of issues including prohibiting retailers from making retrospective adjustments to terms and conditions of supply and holding suppliers liable for shrinkage losses.

Compliance with the Code will be supervised and enforced by the Groceries Supply Code of Practice Ombudsman, which will be a newly created role.

Security Breaches

AVOID CARRYING THE CAN FOR OTHERS' MISTAKES

HSBC was recently fined over £3m by the FSA for not adequately protecting personal data. This shows that quite apart from the adverse PR and damage to customers'/employees' confidence, such losses can be very costly. Similar to the FSA's powers, the Information Commissioner's Office (ICO) will also soon have powers to fine organisations that commit serious breaches of the Data Protection Act 1998 (the Act). These powers are expected to come into force in April 2010.

In addition to being responsible for your own data security breaches, you could also find yourself liable for breaches by any organisations that process personal data on your behalf (e.g. payroll processors, or less obvious examples such as website hosts). This is because the Act requires you to make up front and ongoing checks as to the measures your processors take to keep data secure. You should also have a written contract in place under which your processor undertakes only to process the data in accordance with your instructions, and to take proper precautions to keep the data secure. If you fail to do this, you are on the hook for any data lost by your processor.

Recent press coverage has highlighted the importance of ensuring that your processor agreement addresses issues such as whether your processor may download personal data onto portable devices. If it can, the personal data should always be encrypted. Another important issue is to ensure that your processor notifies you immediately of any actual or suspected security breach. Often, if action is taken quickly, potential losses, for example, through identity fraud, can be avoided or minimised.

If you have existing processor agreements in place you may want to consider amending them to take account of these recent developments to try to minimise your risks going forward.

Tired of MP's expenses stories?

HOW THE FOIA AFFECTS YOU

Although the dust seems to have settled on the issue of MP's expenses, the recent newspaper revelations were made possible because of Tony Blair's election manifesto promise to make public authorities more transparent and accountable.

One of the results of this promise, the Freedom of Information Act 2000 (FOIA), gives anyone (anywhere in the world) the right to request information from a public authority, which includes all central and local government, the NHS, police and schools.

The use of the right to request information costs nothing (except that the request must be made in writing) and might result in the release of useful and valuable information, for example, upcoming business opportunities and tenders.

Clearly, the FOIA presents a risk as well as an opportunity to the private sector, as any information held by a public authority may be disclosed to others if requested. A public authority has an obligation to disclose information requested unless there is a relevant exemption. Having said this, the exemptions are narrow and the overriding principle is that the public authority must disclose. In practice this means that you should be careful which information you provide to public authorities and, if it is confidential, you should take steps to ensure that the public authority is aware of its confidential nature. Whilst this will not guarantee that your information will not be disclosed, it will at least raise the question in the public authority's mind if asked to disclose it.

Age verification: not just a tick box exercise

A new Bill, aimed at reducing the amount of underage customers escaping ID checks by buying age-restricted products online, is currently making its way through Parliament. Retailers will be required to take "all reasonable steps" to ensure that every customer meets any age restrictions. Those who fail to do so will face criminal charges and a hefty fine. Should the Bill become law, in addition to the extensive data protection issues that will arise, the sophisticated software necessary to comply is likely to leave more than a large dent in the petty cash. We will keep you posted.

FOR COMMENTS OR FURTHER INFORMATION CONTACT:

Vicky Wilkes
T: 0121 222 3518
E: vicky.wilkes@hammonds.com

Stuart James
T: 0121 222 3645
E: stuart.james@hammonds.com

Sally Jones
T: 0121 222 3444
E: sally.jones@hammonds.com

And now the team news...

Tough guy Sam

Our very own tough guy, Sam Tibbetts, took part in the Tough Guy challenge in July this year, completing the course in 2hrs 32 minutes and coming a respectable 323rd out of over 2,500 competitors.

As you can see from the photographs, the 8 mile assault course is spread across the muddiest countryside Wolverhampton has to offer. The ever trustworthy Wikipedia notes that running the course involves risking barbed wire, cuts, scrapes, burns, dehydration, hypothermia, acrophobia (fear of heights), claustrophobia, sprains, twists, joint dislocation, broken bones and...death. They forgot to mention the electric wires.

Sam did this for charity and not for the love of pain with donations going to Cancer Research and Sports 4 Life. Sam will be taking it easy for the rest of the year but Stuart James who is going for a PB in the Birmingham Half Marathon and Delizia Diaz who is training hard for the Warwickshire Triathlon intend to make sure that the Commercial Team maintains its status as one of the most dynamic teams at Hammonds.