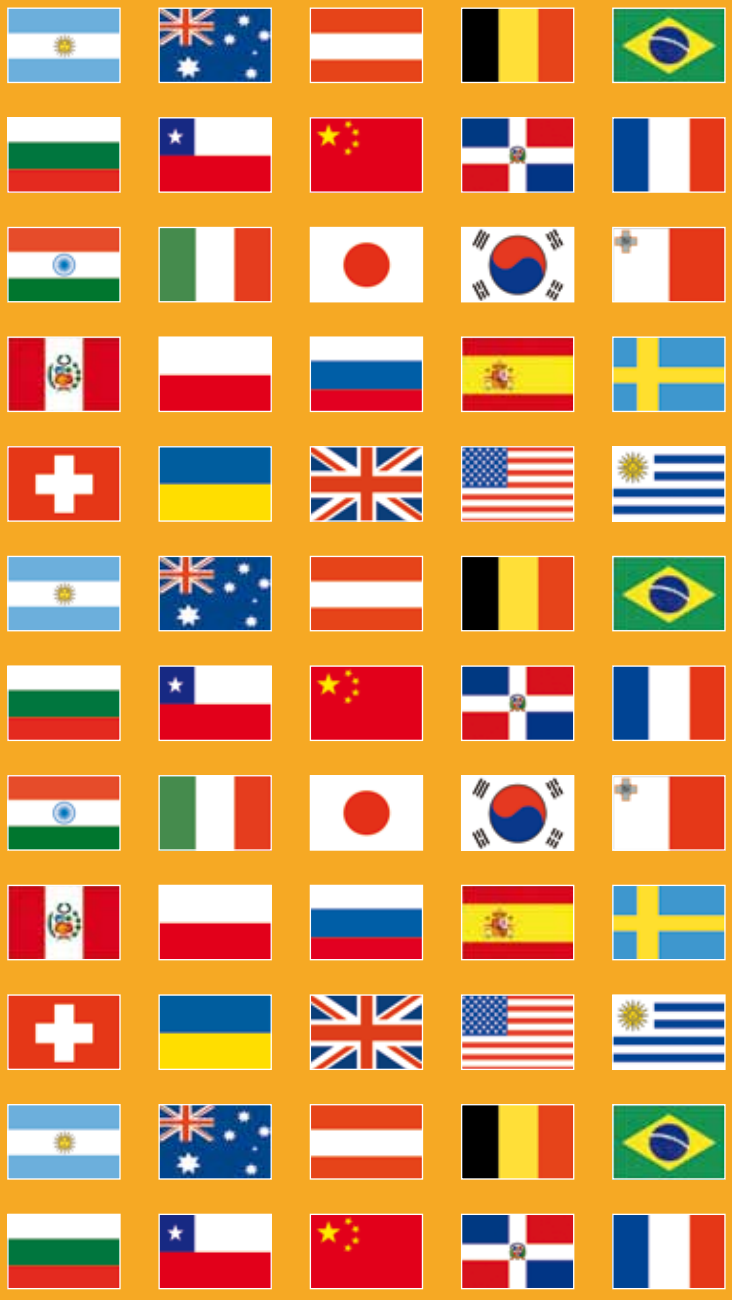
GETTING THE DEAL THROUGH

e-Commerce

in 25 jurisdictions worldwide

Contributing editor: Robert Bond

2013



Published by
Getting the Deal Through
in association with:

Addisons

Altius

Angeles & Lugo Lovatón

Barretto Ferreira, Kujawski e Brancher (BKBG)

Dimitrov, Petrov & Co

Dr Widmer & Partners, Attorneys-at-Law

Ferrere

Foyen Advokatfirma AB

García Magliona y Cia Limitada Abogados

Hankyul Law Firm

Iriarte & Asociados

Karniol Małecki i Wspólnicy Sp.k.

Kochhar & Co

Latournerie Wolfrom & Associés

Martí & Associats

Maybach Görg Lenneis & Partner

Noerr TOV

Orsingher Avvocati Associati

Robins, Kaplan, Miller & Ciresi LLP

Russin & Vecchi LLC

Speechly Bircham LLP

Vitale, Manoff & Feilbogen

WH Partners

Yuasa and Hara

Zhong Lun Law Firm

GETTING THE DEAL THROUGH®

e-Commerce 2013

Contributing editor
Robert Bond
Speechly Bircham LLP

Business development managers
Alan Lee
George Ingledew
Robyn Hetherington
Dan White

Marketing manager
Alice Hazard
Marketing assistants
William Bentley
Zosia Demkowicz

Subscriptions manager
Rachel Nurse
Subscriptions@GettingTheDealThrough.com

Assistant editor
Adam Myers
Editorial assistant
Lydia Gerges

Senior production editor
Jonathan Cowie

Chief subeditor
Jonathan Allen
Production editor
John Harris
Subeditors
Davet Hyland
Caroline Rawson

Editor-in-chief
Callum Campbell
Publisher
Richard Davey

e-Commerce 2013
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2000
Ninth edition 2012
ISSN 1473-0065

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Law Business Research

FSC www.fsc.org MIX Paper from responsible sources FSC®

CONTENTS

United Kingdom

Robert Bond
Speechly Bircham LLP

General

1 How can the government's attitude and approach to internet issues best be described?

The UK government's attitude to the internet could generally be described as favourable, with the government recognising the opportunities for wealth creation, among other benefits. A new team has been set up within the Cabinet Office called 'The Government Digital Service', which is tasked with transforming government digital services. The aim of the team is to enable the government itself to become digital in thinking in order to deliver services which are suitable for users. It has various ongoing projects, including a project entitled 'Assisted Digital', which aims at assisting disadvantaged/vulnerable people who are reliant on public services make the most of internet services.

The internet does, however, pose a number of serious challenges that the government is having to deal with. These challenges arise from the ease and speed with which information can be transferred online and the difficulties for laws to keep pace with technological changes. The government's approach is generally to seek to strike a balance between the rights of individuals to go about their business in the manner they choose and the rights of the public to be protected against unscrupulous practices. The government could generally be said to have embraced the internet, however.

The government introduced the Digital Rights Act 2010 (the DRA), which deals with, among other things, online infringement of copyright. Section 3 of the DRA places an obligation on copyright owners to notify internet service providers (ISPs) of any copyright infringements using a 'copyright infringement report'. After the copyright owner informs an ISP of an infringement, the ISP must then inform the infringing subscriber within a period of one month. The DRA also permits the Office of Communications (Ofcom) to limit or cut off internet access of a subscriber who has infringed copyright habitually with the download of films or music illegally. It is thought that the DRA focuses on peer-to-peer file-sharing rather than copyright law infringement. Ofcom also has the power to impose fines on ISPs who do not take action against persistent offenders. The DRA further allows for the 'sharing of costs' under section 15, whereby the government may order a provision to be included in any code relating to costs incurred under the copyright infringement provisions. This would require the payment of contributions by copyright owners, ISPs and those involved with subscriber appeals.

Since the DRA took effect, it has been criticised by ISPs who feel that it is a threat to customers' basic rights and freedoms in the way that it makes ISPs enforcers and bypasses the courts. ISPs also find the DRA onerous and costly to them in respect of their new enforcement obligations. TalkTalk and BT sought judicial review of the DRA earlier this year on the grounds that it infringed users' internet privacy, was not proportionate and would not work effectively. The appeal was rejected by the High Court, which represents a firm affirmation of the DRA by the courts.

The government has taken the view in relation to the implementation of the E-privacy Directive in the United Kingdom (see question 25) to work with businesses to obtain a workable solution that is not overly prejudicial to UK businesses.

Legislation

2 What legislation governs business on the internet?

UK legislation such as the Sale of Goods Act 1979 (as amended) will apply equally to sales of goods made on the internet as to goods bought through other channels, as will the EU-derived Unfair Terms in Consumer Contracts Regulations 1999 and the Consumer Protection from Unfair Trading Regulations 2008. Acts such as the Unfair Contract Terms Act 1977 will also apply equally to contracts concluded on the internet. Other key acts that are relevant to business conducted on the internet are the Data Protection Act 1998, the Electronic Communications Act 2000 and the Regulation of Investigatory Powers Act 2000.

In addition, the UK government has implemented a number of EU Directives that govern business on the internet. These include:

- the Consumer Protection (Distance Selling) Regulations 2000 (as amended), the purpose of which is to encourage cross-border trade and internet sales by providing additional consumer rights to consumers purchasing goods other than in face-to-face transactions. At the heart of the Regulations are requirements relating to information to be provided to consumers before a transaction is concluded to enable informed buying decisions and a right for consumers to cancel most contracts within a certain period;
- the Electronic Commerce (EC Directive) Regulations 2002, which provide for certain information to be made available to consumers and for such information to be available easily and directly, and to be permanently accessible;
- the Financial Services (Distance Marketing) Regulations 2004 relating to the supply of financial services at a distance; and
- the Privacy and Electronic Communications (EC) Directive Regulations 2003 which regulate unsolicited direct marketing messages.

Other developments of note regarding consumer issues include the Injunctions Directive permitting the OFT to take proceedings in another EEA country if a business is harming the collective interests of UK consumers by breaching European consumer protection laws, and the Consumer Protection Co-Operation Regulation, which came into force in December 2006. This grants national consumer protection authorities in Europe greater powers to protect consumers against breaches of consumer protection laws.

The Distance Marketing of Financial Services Directive establishes a set of EU-wide rules on the information that must be supplied to consumers when financial services are sold at a distance.

The Financial Services (Distance Marketing) Regulations 2004 which implement the Directive came into force in October 2004.

In addition, criminal and defamation laws apply to activities on the internet.

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of e-commerce and internet access tariffs and charges?

No regulatory body has overall responsibility for the regulation of e-commerce as such, although a number of such bodies have interests in ensuring the enforcement of certain laws that apply to e-commerce, for example the information commissioner is as much concerned with ensuring compliance with online privacy issues as with offline issues. In addition, the Trading Standards Institute is as concerned with protecting consumers against online rogue traders, as it is with offline traders.

Ofcom (the Office of Communications) is the regulatory body responsible for ensuring competitive behaviour relating to access tariffs and charges. Ofcom's responsibilities are set out in the Communications Act 2003 (the 2003 Act), and Ofcom also has powers under the Competition Act 1998 (the 1998 Act), the Enterprise Act 2002 (the 2002 Act), and under EU competition law to deal with anti-competitive behaviour. Pursuant to a market review by Ofcom in 2005, British Telecom gave a number of undertakings relating to the price of wholesale broadband services.

Ofcom's powers were significantly increased by the Digital Rights Act 2010, which amended the Communications Act 2003. Ofcom has the right to limit or cut off internet access of a subscriber who has habitually infringed copyright, with the download of films or music illegally.

The UK Information Commissioner's Office (ICO) is the regulatory body associated with data protection. In relation to online activity, the remit of the ICO includes the monitoring of unsolicited marketing material by electronic mail (this includes texts, picture messages and e-mails), which should only be sent if the person has chosen to receive them, unless the e-mail address was obtained as a result of a commercial relationship. The individual should always be given the opportunity to stop receiving the e-mails. Further to the implementation of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, it also includes ensuring that web hosts now obtain consent from users before using cookies, and taking enforcement action when web hosts are in breach (see question 25).

Jurisdiction

4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions (or disputes) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Issues of jurisdiction for internet-based transactions are governed by existing rules of private international law embodied with regard to disputes between EU consumers and businesses within the Rome Convention and Brussels Regulation, incorporated into UK law by the Contracts (Applicable Law) Act 1990 and the Civil Jurisdiction and Judgments Order 2001 respectively.

In the context of consumer issues involving sellers located within the European Union, the broad intention is that European consumers that purchase products from a business in another EU country which has been marketing its products to them should be entitled to the mandatory protections of their own country's consumer laws and have the dispute heard before the courts of their own country, regardless of what the business might state in its terms and conditions. The rules are, however, complex and what law applies and where a claim can be brought will depend on the facts of each case.

With regard to disputes that involve sellers that are not located within the EU, the general position is that the contract will be governed by the law provided in the terms and conditions.

The Rome Convention applies to contractual obligations where a choice of law is involved, even in some cases where the law it designates is that of a non-contracting state. The signatories to a contract may choose the law applicable to the whole or a part of the contract, and select the court that will have jurisdiction over disputes. By mutual agreement they may change the law applicable to the contract at any time (principle of freedom of choice).

Regulation (EC) No. 864/2007 on the Law Applicable to Non-Contractual Obligations (Rome II) was enacted in January 2009. It applies to non-contractual obligations arising in civil and commercial matters. The general rule is that the law applicable to non-contractual obligations is the law of the country in which the damage occurs, or is likely to occur.

Contracting on the internet

5 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

Yes, it is possible to form and conclude contracts electronically. Standard English law contract principles of offer and acceptance apply equally to contracts formed electronically. In order to avoid possible demand issues, it is important that people selling online structure their sites in a way that ensures that the site content is not viewed as an 'offer' that can be accepted by any buyer, but rather as an 'invitation to treat' (eg, like a shop window). The buyer is then the party that makes the offer that the seller is at liberty to accept or reject. This can be an important distinction in cases of pricing errors.

In order to avoid issues regarding whether or not acceptance has actually taken place, at which time a contract is in force between the parties, the Electronic Commerce Directive 2002 (the Directive) as implemented in the UK will apply to internet contracts to ensure that when placing an order on the internet, a receipt is provided and the customer has the opportunity to identify and correct errors prior to placing the order. It is also a requirement of the Directive that the service provider provides terms and conditions applicable to the contract to the customer in a way that the customer may store and reproduce them.

Most websites seek to enforce terms and conditions of use on users by means of a 'click wrap' or 'click through' contract, usually in the form of a screen containing the terms and conditions of use which are available to read and to either accept or reject.

The click wrap concept follows the shrink wrap contract or licence that has been commonly used in the software industry since the 1980s. Two cases in 1996, *Beta Computers (Europe) Limited v Adobe Systems (Europe) Limited* under Scottish law and *Pro CD Inc v Zeidenberg* under US law, have both enforced the validity of shrink wrap licence agreements, provided the customer has the opportunity to read and if necessary reject the terms by returning the product within a reasonable period. In the case of click wrap contracts, the same principles need to apply.

The Unfair Contract Terms Act 1977 (as amended) will apply to the click wrap terms and conditions so that any terms must be fair and reasonable, particularly those that seek to limit liability, and the Electronic Commerce Directive 2002 as implemented in the UK will also apply, as well as the Consumer (Distance Selling) Regulations 2000.

6 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

In addition to English common law principles that apply to contracting on the internet, the main laws that govern contracting on the internet

have been mentioned above and several of them specifically relate to business-to-consumer transactions while not applying to business-to-business transactions, an example being the Consumer Protection (Distance Selling) Regulations 2000, where the 'consumer' must be a natural person who is acting for purposes which are outside his business. The Electronic Commerce Regulations 2002 also apply to contracting on the internet; however, they apply to any natural person who is acting for purposes other than those of his trade, business or profession.

The Unfair Contract Terms Act 1977 can apply to consumer-to-business contracts and also to business-to-business contracts, provided that one party deals 'on the other's written standard terms of business.

7 How does the law recognise or define digital or e-signatures?

Section 7(1) of the Electronic Communications Act 2000, the act which implements the Electronic Signatures Directive 1999/93/EC, defines an electronic signature as anything in electronic form which is incorporated into or otherwise logically associated with any electronic communication or electronic data, and which purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both. Section 7(1) of the 2000 act provides that an electronic signature, or the certification by any person of such a signature, is admissible as evidence in relation to any question as to the authenticity or integrity of a particular electronic communication or particular electronic data. It is for the courts to decide in each case whether an electronic signature has been correctly used and what weight should be attributed to it.

The Electronic Signatures Regulations 2002 define an 'advanced electronic signature' as an electronic signature which is uniquely linked to the signatory, is capable of identifying the signatory, is created using means that the signatory can maintain under his or her sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

It is noteworthy that on 4 June 2012, the European Commission adopted a proposal for a new regulation regarding electronic identification, signatures and trust services (the Proposed Regulation). The key elements of the Proposed Regulation are as follows:

- To upgrade the legal framework of electronic signatures, replacing the existing e-Signature Directive. For instance, it allows you to 'sign' with a mobile phone; it requires higher accountability for security; and it provides clear and stronger rules for the supervision of e-signature and related services.
- Other trust services (ie, services which create, verify and handle electronic signatures, seals, time stamps, delivery services, etc) are included for the first time, meaning that there will be a clear legal framework and more safeguards through strong supervision services of electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.
- Article 15 introduces an obligation for trust service providers to implement appropriate technical and organisational measures for the security of their activities. Furthermore, the competent supervisory bodies and other relevant authorities must be informed of any security breaches within 24 hours. If appropriate, they will inform other member states' supervisory bodies and the individuals affected.
- Trust service providers will be required to employ staff who are trained in data protection law to ensure compliance with the Data Protection Directive.

The Proposed Regulation is now going through the ordinary legislative procedure for its adoption by co-decision of the European Parliament and the Council. It then expected to be in force within 20 days from the date of its publication.

8 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

There are no particular data retention or software legacy requirements in relation to the formation of electronic contracts. Each party is, however, well advised to maintain an audit trail in the event of a dispute arising as to the terms of the contract or its performance.

Security

9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions?

No specific legislation has been enacted with regard to guaranteeing the security of internet transactions, although common law principles and non-internet-specific legislation may apply. A company that loses or permits unauthorised third-party access to customer data may, for example, face a claim for negligence, breach of contract (if there was a contractual term to take care of such data) and a claim under the Data Protection Act 1998, on the basis that such loss or unauthorised access is likely to be a breach of the seventh data protection principle that requires a data controller to take appropriate technological and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss of personal data.

The British Standard, BS 10012:2009 provides a specification for a personal information management system. This standard provides guidance on how to maintain and improve compliance with the Data Protection Act 1998. Although not specifically targeted at internet transactions, it is the first standard produced for the management of personal information.

10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

The key legislation in this regard is the Regulation of Investigatory Powers Act 2000 (RIPA). Part III of RIPA provides a statutory framework, subject to independent oversight, enabling public authorities to require protected information (electronic material that cannot be accessed or put into an intelligible form without a key) which they have lawfully obtained or are likely to lawfully obtain to be put into an intelligible form, to acquire the means to gain access to protected information and to acquire the means to put protected data into an intelligible form. The power may only be exercised with proper and specific permission from a judicial authority and disclosure of a key requires additional requirements to be met. Part III came into force in the UK on 1 October 2007. Under the Code of Practice, the National Technical Assistance Centre is given a specific role to act as a gatekeeper of the part III powers.

The provisions in the Electronic Communications Act 2000 regarding the establishment of an approvals regime for businesses providing cryptography services have not been brought into force. They were repealed on 25 May 2005, which was the cut-off point for the establishment of an approvals regime. The independent, non-profit-making, industry-led body set up to approve new commercial security services, generally called 'trust services', and to provide confidence to consumers is called Scheme.

Pursuant to the Electronic Signatures Regulations 2002, the secretary of state must keep the activities of certification authorities under review and must maintain and publish a register of certification authorities who are established in the UK. Under section 4 of the 2002 Regulations, where a person suffers loss as a result of reasonable reliance on a 'qualified certificate' (a certificate meeting the requirements of the Regulations and issued or guaranteed by an authority meeting the requirements of the Regulations), liability is effectively strict in that negligence is assumed unless the authority can prove otherwise.

Domain names

11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

The rules for the registration and use of domain names within the '.uk' domain and its subdomains are administered by Nominet UK. Applications to register a domain name will generally be made on behalf of an applicant by a registrar (generally an ISP or registration agent). Prices will vary depending on which registrar is used and registrations are for two-year periods before renewal is required. Domain names can be transferred from one entity to another, subject to payment of a fee (at present £11 plus VAT) to Nominet UK.

It is possible to register a '.uk' domain name without being resident in the UK, subject to certain restrictions in respect of '.plc.uk' and '.ltd.uk' names, where the registrant must be either a private or public company registered as such with Companies House.

12 Do domain names confer any additional rights (for instance in relation to trademarks or passing off) beyond the rights that naturally vest in the domain name?

Domain names in themselves do not provide a great deal of protection against third parties using the same or similar names, particularly when initially registered, when no goodwill may have attached to a particular name. If, however, the domain name is also the registrant's trademark, then evidence as to visitor numbers to the domain name in an infringement or opposition action against a third party would be useful. In the absence of a registered trademark, or as an additional claim in a trademark infringement claim, it is conceivable that the owner of a particularly well-known domain name might be able to establish sufficient reputation in a domain name to successfully bring a passing-off claim if a third party's use of a well-known domain name was such as to lead the public into the erroneous belief that there is a connection between the domain name owner and the third party.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Yes, depending on the precise circumstances of each case and the way in which the 'pirate' conducts itself, it may well have a bearing on the outcome. In *British Telecommunications v One in a Million* [1999], several owners of well-known trademarks were successful in bringing a passing-off claim on the grounds that the registration of the domain name and the subsequent offer of sale to the claimants made a false representation that the defendant was associated with the claimant, and potentially raised the prospect of damage to the claimants if they did not purchase the domain names offered to them. In the same case, with regard to trademark infringement, the court ruled that the defendant's use of the claimants' well-known trademarks (which had a reputation in the UK) was detrimental to the reputation of the marks and amounted to trademark infringement under the Trade Marks Act 1994. There are other examples of successful claims by trademark owners, although it is worth noting that there have also been cases where the courts have found that a domain name registrant has a perfectly legitimate right to register a domain name, particularly where the goods and services differed from those of the trademark owners and there was therefore no likelihood of confusion.

As an option to court action, a trademark owner may decide to use the more informal procedures offered by Internet Corporation for Assigned Names and Numbers (ICANN) with respect to top-level domain names or Nominet UK in respect of '.uk' domain names. This is often a cheaper and quicker route to resolution than court action and can be particularly useful where the aim is to achieve transfer of the domain name rather than pursue damages.

Advertising

14 What rules govern advertising on the internet?

Advertising on the internet is governed by the same rules that apply to other advertising channels, although the reach of the internet poses potential problems for advertisers where their adverts may be viewed further afield than might be intended. Advertisers would be well advised to clearly state at which jurisdiction their adverts are aimed.

In the UK, advertisers need to comply with the Business Protection from Misleading Marketing Regulations 2008 (BPMMR) which prohibit misleading advertising to businesses and establish when comparative advertising will be allowed. Advertisers also need to comply with the Consumer Protection from Unfair Trading Regulations 2008 (CPUTR) under which commercial communications made to consumers that are misleading or aggressive are prohibited.

Additionally, advertisers need to comply with the British Codes of Advertising, Sales Promotion and Direct Marketing (as published by the Committee of Advertising Practice and known as the CAP Code) that have been found to apply to internet activities. The Advertising Standards Authority has responsibility for enforcing the CAP Code. Further, specific rules on advertising apply to certain specific sectors, such as the financial services sector.

CAP clarified the existing online remit of the code, which covers paid-for advertisements and sales promotions on websites. New CAP and BCAP UK advertising codes came into effect on 1 September 2010, introducing greater clarity and consistency in the codes. There is a particular focus on children and their enhanced protection in relation to advertising. There is also a change in the approach taken with regard to environmental claims, nutrition and health claims made on foods. CAP and BCAP have also provided guidance on specific sectors such as comparative charity ads, adult material and betting tipsters. From March 2011, the content of organisations' own websites together with advertising and marketing on social networking sites also fall within the scope of the CAP Code.

Certain legislation specific to certain activities may also contain provisions relating to advertising. The Gambling Act is an example and contains specific rules relating to the advertising of gambling activities (see question 15).

15 Are there any products or services that may not be advertised or types of content that are not permitted on the internet?

While no products are entirely banned from advertisement on the internet, UK laws regulating advertisements for (among others) alcohol, tobacco and prescription drugs will apply to the internet. Tobacco advertising is in particular heavily regulated by the Tobacco Advertising and Promotion Act 2002 and the exceptions to a general prohibition are limited. Additionally, the Advertising Standards Authority has published new rules as part of the British Code of Advertising, Sales Promotion and Direct Marketing relating to non-broadcast advertisements for food or soft drink products aimed at children (effective 1 September 2010) and non-broadcast advertisements relating to gambling (effective 1 September 2007) with the implementation of the Gambling Act 2005. Such advertisements are not banned but must satisfy certain requirements of the code. In particular, marketing communications to children must not encourage or otherwise condone poor nutritional habits or an unhealthy lifestyle in children. Gambling marketing must also ensure that the marketing is socially responsible, with a particular responsibility to persons under 18, children and other vulnerable persons.

Financial services

16 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

Pursuant to the Financial Services and Markets Act 2000 the Financial Services Authority (FSA) regulates most types of firms selling financial services in the UK, including on the internet, although the FSA does not regulate the selling of loans, credit cards, occupational pension schemes or day-to-day banking services, which are regulated by Trading Standards, the OFT, the Pensions Regulator and the Banking Code Standards Board. By law most financial services business operating in the UK require authorisation from the FSA.

Companies advertising financial products or services must ensure that their adverts (which can include e-mails and websites) are clear and fair and do not mislead customers. The FSA has the power to require companies that produce misleading adverts to (among other things) withdraw the advert, publicly warn the company involved or issue a fine. Matters concerning 'non-technical' elements of financial advertisement, such as taste and decency or social responsibility, are regulated by the Advertising Standards Authority (ASA).

Customers are encouraged to report misleading adverts and unfair terms in customer contracts to the FSA.

A key piece of legislation regarding the online marketing of financial services in the UK is the Financial Services (Distance Marketing) Regulations, which came into effect in October 2004 and implemented the 2002 EU Directive on the Distance Marketing of Financial Services. The Regulations only apply to consumer contracts concluded at a distance and require the supplier to disclose certain information, including the supplier's geographical address and particulars of any supervisory body (eg, the FSA) with a link to their website, together with information as to the product details and the terms of the contract, including right to cancel and payment details. Consumers have the right to cancel without incurring liability within a specified cooling off period in most cases (but not all), the length of which will depend on the nature of the product. The information required must be provided to the consumer in a clear and comprehensible manner on paper or another appropriate durable medium before the contract can be concluded. The supplier must provide a copy of its terms and conditions prior to conclusion of the contract.

The Consumer Credit (Advertising) Regulations 2004 came into force on 31 October 2004 and made important changes to the regime governing the contents of advertisements for credit, loan or hire products, including advertisements for such products on the internet.

Defamation

17 Are ISPs liable for content displayed on their sites?

In *Godfrey v Demon Internet* [1998], Demon (an ISP) was held liable for defamatory material that it failed to remove for a period of 10 days after being advised that the material was defamatory. ISPs should therefore remove material that might be defamatory as soon as possible on being informed of such material. The Electronic Commerce (EC Directive) Regulations 2002 (enacting the E-Commerce Directive) seek to provide some comfort for ISPs in relation to defamatory content of which it is not aware and provides that ISPs will not be liable for such material as long as they did not initiate the transmission and they remove the material once they have received a complaint.

The 2002 Regulations also provide protection for ISPs against claims of copyright infringement as a result of caching sites subject to certain conditions. Further, an ISP will not be liable for unlawful content stored at the request of a user of its services provided that the ISP acts expeditiously to remove or disable such material once it has actual knowledge of it.

ISPs are not under any general duty to monitor content of the materials held or transmitted through its services.

18 Can an ISP shut down a web page containing defamatory material without court authorisation?

The best way for an ISP to avoid arguments that it has no right to remove such material is to have clear terms and conditions in place that state that the ISP has such rights of removal, even in the case of an allegation of defamation, although an ISP would be best advised to investigate the matter quickly and thoroughly before taking such action. The ISP may also wish to consider including in its terms an indemnity in its favour if damages are sought against it as part of a defamation claim.

Intellectual property

19 Can a website owner link to third-party websites without permission?

This issue has become a key battleground in recent years with the advent of sites such as youtube.com which enable users to upload copyright content onto the website provider's site for viewing by others. Several actions have been launched in other jurisdictions (most notably the US) and the UK will watch these cases with interest, as many of the issues in contention will be the same in the UK. The key question is whether the website provider's defence that it is merely a platform will be effective.

The issues with regard to third-party content used on the internet will be the same as if they were used in other contexts, the primary question being whether the third-party content in issue is protected by copyright (or possibly other rights such as database, trademark or design rights). If the content being used is protected by copyright (or other rights), then use without permission will, subject to certain limited exceptions and assuming that such use amounts to the copying of the whole or a substantial part of the copyright work or otherwise constitutes an act that is reserved for the copyright owner and his or her authorised users, be an infringement and expose the website provider to a claim for copyright infringement.

20 Can a website owner use third-party content on its website without permission from the third-party content provider?

Case law in this area is undeveloped but the general view is that linking without permission from one homepage to another homepage where there is no copying of any copyright material is acceptable, although the owner of a linked site could theoretically claim that a link causes a breach of the 'making available right' introduced into UK law by the Copyright and Related Rights Regulations 2003 if it could be shown that the link constitutes an 'electronic transmission in such a way that members of the public may access [the copyright work] from a place and a time individually chosen by them'. The party creating the link should also bear passing-off and trademark issues in mind when creating the link and should make it clear that the user is leaving one site and going to another. Linking in breach of a contractual obligation not to do so might also constitute a breach of contract.

Deep linking (bypassing the homepage of the linked site) raises similar concerns for sites linked without permission. Arguments have been run successfully against deep linking in other EU jurisdictions based on infringement of database rights. A claimant would need to show that the relevant pages on its website constituted a database and that the link made the database available in a manner that constituted reutilisation.

'Framing' is the practice of displaying content from another website within the frame or border of a website. As framing involves copying another party's content, the risk of a copyright infringement claim is greater than with linking if the framed content constitutes a substantial part of the framed website's copyright material.

Additionally, depending on the precise circumstances of the case, the framing party potentially runs the risk of a passing-off claim, a trademark infringement claim, a database rights infringement claim and a breach of contract claim.

A further issue that has been of interest in this respect in the UK is the use of 'metatags' (also known as 'keywords') whereby website providers seek to drive traffic to their sites by the use of other party's trademarks in the embedded code of their sites that is then picked up by a search engine searching against that term. In the case of *Reed Executive v Reed Business Information* [2004], the English courts held that the use of a registered trademark or a similar mark in a metatag does not necessarily constitute trademark infringement or give rise to a passing-off claim and the court questioned whether a metatag could constitute use of a trademark at all. A certain amount of care needs to be taken in this regard, however, and a trademark owner who feels that its marks are being taken advantage of may wish to complain to the search engine in question, even if it decides not to take more formal legal action.

21 Can a website owner exploit the software used for a website by licensing the software to third parties?

This will largely depend on who owns the copyright (and, if relevant, the database rights) in the relevant software, and if it is licensed in by the website provider, and whether sub-licensing is permitted by the terms of its licence.

If the website provider is not the owner of the rights in the software and it is not expressly permitted to sub-license the software to a third party, then such sub-licensing may expose the website provider to a claim for breach of contract and a copyright (and possibly database rights) infringement claim, as well as expose the purported sub-licensee to a copyright (and possibly database rights) infringement claim by the actual owner(s) of such rights.

22 Are any liabilities incurred by links to third-party websites?

Website providers providing links to third-party websites will generally provide an express statement at the point of the link stating that the user is moving from one site to another and that no liability is accepted for the content of the site being linked to or for the user's use of the linked site. There has not been any case law to date as to whether such an exclusion of liability would protect the linking site from damage suffered by the user through the user's use of the linked site. The question to be answered would most likely be whether such an exclusion was reasonable under the Unfair Contract Terms Act 1977 and additionally where the user is a consumer whether the exclusion was fair and reasonable under the Unfair Terms in Consumer Contracts Regulations 1999.

As noted above the link itself could give rise to a trademark infringement or other claims by the owner of the site to which a link is provided.

Data protection and privacy

23 How does the law in your jurisdiction define 'personal data'?

The Data Protection Act 1998 (DPA), which implemented the 1995 EC Data Protection Directive, is the legislation that defines 'personal data' in the UK. The DPA replaced and expanded upon the 1984 Act of the same name.

'Personal data' is defined as data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession or is likely to come into the possession of the data controller.

'Sensitive personal data' means personal data consisting of information as to the racial or ethnic origin of the data subject, his or her political opinions, religious beliefs or other beliefs of a similar nature, whether he or she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), his or her physical or mental health or condition, sexual life, the commission or alleged commission by him or her of any offence, or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings. However, if the general draft data protection regulation (the Draft Regulation), which is currently being debated, is enacted in its current form, 'sensitive data' will also includes 'biometric' data.

Since the decision in *Durant v Financial Services Authority* [2003], the position in England and Wales has been that to qualify as personal data, data must have the data subject as their focus and be of a biographical nature, meaning that which goes beyond merely stating the data subject's involvement in a matter or an event that has no personal connection to the data subject. This was confirmed in *Smith v Lloyds TSB Bank plc* [2005] where documents held by Lloyds and the information contained within the documents were not personal to Smith in the relevant sense, but all files related to loans to Lloyds. It was held that as there were no personal data in the files, it was merely the case that Mr Smith was mentioned in files; however, he acted on behalf of his company rather than the data being biographical information about him.

However in 2007, the Article 29 Working Party issued an opinion stating that the definition of 'personal data' should be interpreted widely. This position was reiterated in guidance published by the ICO later on in 2007.

24 Does a website owner have to register with any controlling body to process personal data? May a website provider sell personal data about website users to third parties?

Subject to certain limited exemptions, the DPA requires every data controller (the person who determines the purpose and manner of processing of personal data) to register as such with the ICO. The ICO maintains a public register (accessible online) which gives the name and address of the data controller together with a general description of the processing carried out by the data controller. It is a criminal offence for a data controller not to register and the potential fines far outweigh the limited annual registration fee. Completing the application form is straightforward and can be done online.

A breach of the DPA can result in a fine of up to £500,000 if the information commissioner is satisfied that there has been a serious contravention of section 4(4) of the act by the data controller; the contravention was of a kind likely to cause substantial damage or substantial distress and either the contravention was deliberate; or the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention. Under the Draft Regulation, the maximum fine for a breach of the regulation will be €1 million or 2 per cent of a company's annual worldwide turnover.

Companies which are FSA-regulated should also be aware that the FSA can impose unlimited fines for data breaches; the highest fine imposed to date was £2.275 million for data security failings by Zurich UK.

A website provider that wishes to sell a database must ensure that in doing so it complies with the principles of the DPA, in particular processing must be fair and lawful and for specified lawful purposes. The best way to ensure that these principles are met on a sale of a database will be to include an express statement in the website's privacy policy stating that sale of the database to a third party is a possibility, whether as a sale of the website provider or as part of the website operator's general business. Further, where sale is to a third party for the direct marketing purposes of the third party, the website provider should seek an explicit consent to transfer of data

to a third party for direct marketing purposes. If such consent is not obtained, then the data subject's information should not be included within the database on sale.

25 If a website owner is intending to profile its customer base to target advertising on its website, is this regulated in your jurisdiction? In particular, is there an opt-out or opt-in approach to the use of cookies or similar technologies?

In addition to the DPA, which applies to personal data collected about customers, the Privacy and Electronic Communication Regulations 2003 (PECR) are of importance regarding profiling by website providers of its customer base for advertising purposes. One method of collecting useful information is through the use of cookies, web bugs and other such tracking devices.

On 26 May 2011, the government introduced the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the Regulations) to implement the changes made to the E-privacy Directive at EU level. The Regulations completely change the way that cookies operate on the internet.

Before the change in the law, entities making use of cookies were obliged to inform users that cookies were being used and how they were being used. In general, this information was provided in a website's online privacy policy. Individuals could 'opt out' if they objected to the use of cookies by setting their browser settings in a certain way.

Now a user's informed consent is required for cookies to be used. However, the government has advised in guidance that informed consent does not have to be 'prior consent' as was originally believed by the industry. Rather the definition of consent in article 5(3) is that which is found within the Data Protection Directive (DPD), which is not time-specific. Consent is defined in the DPD as 'any freely given specific and informed indication of his wishes'. As such, while the consent must be informed, there is no indication in the definition as to when that consent may be given. As such the government has confirmed that consent may be given during or even after processing.

For informed consent to be obtained, the user must be presented with clear and comprehensive information of how and why any cookie is being used. Provided that sufficient information is given to the user, consent can be constituted by the user amending their browser settings to constitute consent, or by 'some other method' (new regulation 6(3A)). Note that the ICO has advised that where sufficient information is not provided, that browser systems are not sophisticated enough at present for website hosts to assume that the user has given their consent for the website to use a cookie. The government has, however, given guidance to state that provided that sufficient information is clearly presented to the user (about cookies and what browser setting means for it), in some circumstances the user can actually not amend their browser settings and still be able to signify consent.

The ICO also suggests several factors that will assist the provider as they seek to determine what level of information is necessary in order for them to obtain valid consent; these include the nature of the intended audience of the site and the nature of the site itself. Websites that target more technologically minded visitors may not wish to provide basic information about cookies, but rather a more detailed explanation of how the site puts them to use. In addition, the more prominent the placement of cookie information the more likely it is that the website operator will be able to assume that users understand and accept how the site works.

The ICO emphasised that the key point is that providers should be upfront with users about how their websites operate. They must gain consent by giving the user specific information about what they are agreeing to and providing them with a way to show their acceptance. Any attempt to gain consent that relies on users' ignorance about what they are agreeing to is unlikely to be compliant.

Regulation 6(4)(b) states that consent will not be required where a cookie is 'strictly necessary' to deliver a service which has been explicitly requested by the user. However, the ICO's guidance advises that the exception must be interpreted narrowly. It explains that the use of the phrase 'strictly necessary' means that its application must be limited to a small range of activities, and the use of the cookie must be related to the service requested by the user, for example, the use of a cookie in relation to an online shopping basket. The idea that the services must be 'explicitly requested' by the user means that the narrowing effect of the word 'explicitly' must be borne in mind. This means that the exception would not apply 'just because you have decided that your website is more attractive if you remember users' preferences'.

Note that in relation to third-party behavioural advertising, the ICO advises that if a website uses third-party cookies in third-party behavioural advertising, that the website should 'do everything they can to get the right information to users to allow users to make informed choices about what is stored on their device'. If the information collected on a website is passed on to a third party, this must be disclosed to the user together with any options the user has. The website host should review what the third party does with any information collected.

The ICO states that it will take a practical and proportionate approach to enforcing the rules on cookies. In most cases this will involve the ICO contacting the organisation responsible for setting the cookies, asking them to respond to the complaint and requiring them to explain what steps they have taken to comply with the rules. Those breaches that continue despite the intervention of the ICO or those that are particularly privacy-intrusive are more likely to incur formal action. Where compliance is delayed because the removal of cookies in existing software requires an expensive upgrade, the ICO will expect these costs to be carefully weighed against the intrusiveness of the cookies in question and the length of time that is expected to elapse before the problem is eventually remedied. The ICO has already written to 75 companies asking them to explain the steps they have taken towards compliance.

The PECR places restrictions on how a website provider can carry out unsolicited direct marketing by e-mail, which also apply to any message that consists of text (eg, SMS), voice, sound or images. Under the PECR a website provider can only carry out unsolicited marketing (that is, marketing which has not specifically been asked for) by e-mail if the individual being targeted has given permission, except where the website provider has obtained the individual's details in the course of a sale or the negotiations for a sale of a product or service to that individual, the messages are only marketing similar products or services of the website provider, and the individual is given a simple opportunity to refuse the marketing when their details are collected and, if they do not opt out, the website provider gives the individual a simple way to do so in every future message. The opt-out option should allow the individual to reply directly to the message.

Individuals are entitled to opt out of receiving marketing at any time and website providers must comply with any opt-out requests promptly. Marketing companies must provide details of their identity and a valid address to recipients of marketing material. The rules on e-mail do not apply to e-mails sent to organisations except with regard to the rules as to identity and the provision of an address, although individual's e-mail addresses at an organisation will be subject to the DPA.

With respect to unsolicited direct marketing by third parties by e-mail, this should only be done with the data subject's explicit consent by way of an express opt-in.

26 If an internet company's server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?

A company that collects personal data must comply with the eight principles of the DPA in the way it processes such data, the eighth

principle of which is that personal data should not be transferred to countries outside of the EEA without adequate protection, except in certain specified circumstances, such as where the data subject has consented to the transfer. If the electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country, this does not bring the transfer within the scope of the eighth principle. The obligations for the company in this case will depend on whether it retains control of the server itself, in which case it may be relatively simple to reach a decision as to adequacy, or whether it engages a third party outside the EEA to process data on its behalf where adducing adequacy may require more thought. The two most straightforward ways to achieve adequacy will be to place contractual requirements as to security on the third party, together with restrictions on use of the data by the third party, or to use the model contract clauses approved by the European Commission and the ICO for transfers to organisations acting on a data controller's behalf. These contract terms can be used independently or incorporated into the main contract with the third-party organisation.

27 Does your jurisdiction have data breach notification laws?

Yes, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the Regulations), which took effect on 26 May 2011, introduce new regulation 5A(2) into the Privacy and Electronic Communication Regulations 2003 (PECR), which obliges 'service providers' (providers of public electronic services) to notify any personal data breaches to the ICO without delay. If the personal data breach is likely to adversely affect the personal data or privacy of a subscriber/user, the service provider must also notify that individual concerned. Note that this requirement to notify applies to service providers only. In relation to other entities, ICO guidance states that the ICO expects that any data breaches should be made known to it. Financial services firms may have further obligations to notify the Financial Services Authority of any data breaches.

Taxation

28 Is the sale of online products subject to taxation?

The sale of online products by a UK website operator is generally viewed by the UK taxation authorities as the supply of a service that is subject to value-added tax (VAT), subject to certain thresholds being exceeded. This includes where sales are made from the UK to an EU consumer, and possibly to an EU business depending on whether the EU business is itself VAT registered in its home state when the supplier may be able to zero-rate VAT. Where a UK business's sales exceed a VAT threshold in a member state, the UK business may need to register for VAT in that member state.

With respect to downloads (again treated as services), whether VAT is payable will depend on whether a consideration is paid (in money or in kind) as for a supply of services to take place. As digitised products are regarded as services, certain products that in hard copy form are zero-rated (eg, books) may be subject to VAT when supplied in digitised form.

In respect of certain classes of services provided electronically, a 'reverse charge' procedure operates which deems the place of supply to be where the recipient resides, rather than the location of the supplier. In such cases, the UK supplier would not have to account for VAT on sales to business customers within the EU or outside the EU, but the EU customer would have to account for VAT in its member state. The aim of this provision is to ensure a level playing field for business-to-business transactions whether they take place with customers within the EU or outside the EU.

These provisions also apply in respect of services supplied by a supplier outside the EU, meaning that an EU business customer may have to account for VAT in its member state on such transactions.

The position differs with regard to consumers where the supply will be treated as within the EU if the recipient resides there. Supplies to UK recipients will therefore be subject to UK VAT regardless of where the supplier resides. The current regime permits non-EU-based suppliers to register in the member state of their choice. No VAT is required to be accounted for on supplies to non-EU recipients.

29 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

A UK company placing its servers outside the UK may find itself subject to local tax laws of the country in which it has placed its servers if the laws of the country in question find such servers to constitute a permanent establishment that thereby creates a taxable presence. In certain countries the carrying on of business through a website may constitute a permanent establishment for local law purposes, making the UK company potentially liable to pay tax in that jurisdiction. Even if the servers of a UK tax resident placed outside the UK do not create a permanent establishment for the purposes of the jurisdiction in which the servers are placed, the UK company will still be liable for UK tax on income made through its e-commerce activities.

The UK government's position is presently that neither the operation a website itself nor the location of a server in the UK will constitute a permanent establishment in the UK. The UK's position in this regard is stated in the OECD's Committee on Fiscal Affair's report dated 22 December 2000 entitled 'Clarification on the Application of the Permanent Establishment Definition in E-commerce: Changes to the Commentary on the Model Tax Convention on Article 5'. This is at odds with the views of other countries and it remains to be seen whether this position will be maintained. It should be noted, however, that a permanent establishment could nevertheless exist in the UK if other factors for the creation of such a permanent establishment are met and the position will be fact-specific in each case.

30 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

In the UK, VAT applies to domestic internet sales. Companies making or intending to make taxable supplies of goods or services in the course of or furtherance of a business in the UK must be registered for VAT purposes if the taxable turnover exceeds or is expected to exceed specified limits.

31 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

In these circumstances, unless the goods are re-exported by the recipient, the recipient will not be able to reclaim any VAT and duty paid by the recipient. If the goods are returned to a high street branch of an offshore company, if the high street branch refunds any VAT and import duty paid by the recipient on the original supply by the offshore company, the high street entity may not be able to deduct the refunds for corporation tax purposes.

Gambling

32 Is it permissible to operate an online betting or gaming business from the jurisdiction?

The Gambling Act 2005 (the Act), which came into force in the UK in full from September 2007 and which repeals the Betting, Gaming and Lotteries Act 1963, the Gaming Act 1968 and the Lotteries and Amusements Act 1976, represents a radical shift in gambling

law in the UK. The Act contains specific provisions regulating various technological means by which gambling activities can now be conducted. The Act adopts the concept of 'remote gambling' to cover gambling where the participants are not face-to-face on the same premises, and defines remote gambling to mean gambling where people are participating by means of remote communication, including the internet. Gambling is defined as including gaming and betting.

The Act establishes two comprehensive offences: providing facilities for gambling or using premises for gambling, in either case without the appropriate permission. Such permission may come from a licence, permit or registration granted pursuant to the Act or from an exemption given by the Act. Where authority to provide facilities for gambling is obtained under the Act, it will be subject to varying degrees of regulation, depending on the type of gambling, means by which it is conducted, and people by whom and to whom it is offered.

Persons operating remote gambling sites through the use of equipment situated in Great Britain must obtain a remote gambling licence, by virtue of section 36 of the Act, irrespective of whether the facilities are provided to people in or outside Great Britain.

Section 5(2)(c) provides a general exception for entities such as ISPs (which do no more than act as information carriers) to the offence for providing facilities for gambling without a licence.

Subject to limited exceptions for gaming machines, section 41 makes it an offence to manufacture, supply, install or adapt computer software for remote gambling without an operating licence.

The Act also creates an offence where a person based in Great Britain uses remote gambling equipment to enable a person in a prohibited territory (to be designated by the relevant secretary of state) to participate in remote gambling.

The Act introduces a unified regulator for gambling in Great Britain, the Gambling Commission (the Commission), taking over from the Gaming Board for Great Britain, and a new licensing regime for commercial gambling (to be conducted by the Commission or by licensing authorities, depending on the matter to be licensed). The Act removes from licensing justices all responsibility for granting gaming and betting permissions, which they exercised previously. Instead, the Commission and licensing authorities will share between them responsibility for all matters previously regulated by licensing justices.

The Commission will not regulate spread betting, which is currently the preserve of the Financial Services Authority, or the UK National Lottery, which is regulated by the National Lottery Commission.

The Commission, in addition to assuming responsibility for regulating gaming and certain lotteries, will take on responsibility for regulating betting. The Commission will be responsible for granting operating and personal licences for commercial gambling operators and personnel working in the industry.

The three objectives underpinning the functions of the Commission and licensing authorities are the protection of children and other vulnerable people at risk of being harmed or exploited by gambling; the prevention of gambling from being a source or support of crime or disorder; and the conduct of gambling in a fair and open way.

The House of Commons Select Committee on Culture, Media and Sport launched an inquiry in May 2011 to establish how effective the Gambling Act has been in achieving its aims.

33 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Residents of the UK are permitted to use online casinos and betting websites. One of the key concerns of the Gambling Act is the protection of children and section 46 provides that a person will commit an offence if he or she invites, causes or permits a child (under 16) or a young person (under 18) to gamble. 'Inviting' includes advertising and other actions that bring attention to the facilities available for gambling. Section 63 provides a defence to the offence if the person can prove that all reasonable steps were taken to determine the individual's age and reasonably believed that the person in question was not a child or young person. Section 48 provides that, except in limited circumstances, it is an offence for a young person to gamble.

Section 64 enables the use of children and young persons in test purchasing operations for the purpose of assessing whether underage gambling laws are being complied with.

Outsourcing

34 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

A provider of outsourcing services must ensure that the agreement provides for (as a minimum):

- the definition and scope of the services to be provided;
- the service levels being committed to;
- the potential remedies available for failure to meet such service levels and the agreement in general (including appropriate liability caps);
- change control provisions to properly deal with changes that may arise during the course of the agreement;
- dispute resolution procedures that are sufficiently flexible to enable small-scale disputes to be resolved quickly and informally;
- intellectual property ownership issues;
- choice of law (particularly where the parties are in different jurisdictions); and
- exit management.

The tax issues will differ from deal to deal and will often depend on where the services will be provided.

35 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

The Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) came into force on 6 April 2006, replacing the 1981 Regulations of the same name. TUPE applies to all employers in the UK and cannot be contracted out of. TUPE is intended to protect employees by automatically transferring the employees and associated liabilities to a new employer if the business in which they are employed changes hands. TUPE will apply in most circumstances where an employer outsources or makes a 'service provision change' by engaging a third party to provide services that it previously provided in-house.

TUPE applies when a 'relevant transfer' occurs. A relevant transfer occurs on the transfer of an economic entity which retains its identity. In determining whether a relevant transfer has occurred, the courts will review a number of factors, for example, whether any customers are transferred with a service.

On a relevant transfer, TUPE provides that 'all the transferor's rights, powers, duties and liabilities under or in connection with the transferring employees' contracts of employment are transferred to the transferee'. This includes rights under the employment contract, statutory rights and continuity of employment and includes employees' rights to bring a claim against their employer, for example, for unfair dismissal, redundancy or discrimination. Employees that are transferring do so on their present terms and conditions and without affecting their present rights and liabilities. Except where the new employer can rely on a defence of economical, technical or organisational reason, any dismissals made by the new employer will be automatically unfair where the sole or principal reason for the dismissal is the transfer or a reason connected to the transfer, and the new employer is prohibited from making any changes to the terms and conditions of employment of the transferred employees if the sole or principal reason for the variation is connected to the transfer.

Incoming and outgoing employers have certain specific obligations with regard to employees on a business transfer and must inform and consult representatives of affected employees in sufficient time to enable proper consultation by the outgoing employer. In particular, changes or proposals for changes must be discussed. The incoming employer must supply sufficient information to the outgoing employer to enable the outgoing supplier to comply with its obligations to inform and consult. If the incoming and outgoing employers are found by an employment tribunal to have failed to inform and consult employees, it can award such compensation as it considers just and equitable up to a maximum of 13 weeks' pay per affected employee. Unless the transfer agreement provides otherwise, such liability can be split between the incoming and outgoing employers.

TUPE 2006 introduced a duty on the outgoing employer to provide the incoming employer, no less than 14 days before the transfer, with certain written information regarding the transferring employee (eg, particulars of employment) and details of the rights and liabilities that will transfer. Failure to comply with this duty can expose the outgoing employer to a claim for compensation by the incoming employer.

Online publishing

36 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability?

Mistakes fall short of fraud or deliberate acts or omissions, and whether a publisher itself would be liable may depend on whether the publisher is publishing information on its own behalf or merely in the capacity of a platform provider.

Liability could potentially arise in a number of scenarios and could potentially result in a contractual claim (if a publisher has warranted the information as correct, for example, and loss arises) or a claim for defamation if the mistake related to a living individual. The most likely liability with respect to mistakes, however, is negligence and in particular negligent misstatement in circumstances where a 'special relationship' exists between the parties. For a special relationship to exist, there must be, most importantly, foreseeability of reliance by the representee, sufficient 'proximity' between the parties, and it must be just and reasonable for the law to impose the duty. This may be of concern where bespoke advice is provided on a website.

A publisher could potentially also be liable for negligent misrepresentation under the Misrepresentation Act 1967 where a mistake in information provided on a website induced a person to enter into a contract with the publisher. It could, however, be argued that a mistake falls short of the standard of negligence required to enable such a claim to proceed.

Subject to satisfying tests as to incorporation of a term limiting liability and reasonableness, liability for negligent misstatement and negligent misrepresentation could be limited (although probably not avoided altogether without risk of failing the reasonableness test) by website terms and conditions.

37 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

A database for English law purposes is a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means. Such databases may be protected by copyright or a separate database right, each of which provides certain rights against unauthorised use and reproduction. According to the Copyright and Rights in Databases Regulations 1997, for a database to enjoy copyright protection, the selection or arrangement of the database must amount to an intellectual creation of the author. Database rights may exist in a database where there has been a substantial investment in obtaining, verifying or presenting the contents of the database. Even where a database does not enjoy copyright protection or no database right exists, the website provider could potentially control use of the databases through its terms and conditions.

38 Are there marketing and advertising regulations affecting website providers?

Regulations that apply generally to online advertising and marketing will apply in the same way to website providers; see question 14.

If website providers are making use of third-party online behavioural advertising, they will need to ensure they are complying with their obligations under the Data Protection Act 1998 where acting as data controller. Note that processing of non-obvious identifiers can constitute processing of personal data as this collection and analysis builds a profile of an individual that distinguishes them. See question 25 in relation to online behavioural advertising.

Since 1 March 2011 the CAP Code (the Committee of Advertising Practice Code) has applied to 'advertisements and other marketing communications by or from companies, organisations or sole traders on their own website, or in any non-paid-for space online under their control, that are directly connected with the supply or transfer of goods, services, opportunities and gifts, or which consist of direct solicitations of donations as part of their own fund-raising activities'.

The Advertising Standards Authority in the UK enforces the CAP Code, which now applies to businesses' websites as well as other non-paid-for space such as social networks.

Speechly Bircham LLP

Robert Bond **robert.bond@speechlys.com**

6 New Street Square
London EC4A 3LX
United Kingdom

Tel: +44 20 7427 6400
Fax: +44 20 7427 6600
www.speechlys.com

GETTING THE DEAL THROUGH®

Annual volumes published on:

Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Dispute Resolution
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Insurance & Reinsurance
Intellectual Property & Antitrust
Labour & Employment
Licensing
Life Sciences
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Patents
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Equity
Product Liability
Product Recall
Project Finance
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Shipbuilding
Shipping
Tax on Inbound Investment
Telecoms and Media
Trademarks
Vertical Agreements

For more information or to purchase books, please visit:
www.GettingTheDealThrough.com

ABA Section of International Law
Your Gateway to International Practice

Strategic research partners of the ABA International section

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

INTERNATIONAL BAR ASSOCIATION

The Official Research Partner of the International Bar Association

E-COMMERCE 2013 ISSN 1473-0065