Chapter 4

Data in a Digital World

Introduction

4.1 Web 2.0 is about the personalisation of the internet experience. A noticeable trend associated with this is the way the consumer can set his or her privacy standards on key networking sites such as Facebook. Website privacy policies are also coming under unprecedented public scrutiny – in 2009, Facebook was forced to reverse a change to its policy on ownership of user data within days of a media storm arising around the issue. This may be contrasted with the more traditional view that personal data is just a commodity to be used and transferred globally with minimum compliance with data protection laws.

This chapter:

- reviews the way that personal data is collected in an electronic environment;
- provides an overview of the *Data Protection Directive* is and explains the obligations in respect of cross-border data transfers by service providers;
- examines the meaning of personal data on the internet, including specific issues such as whether Internet Protocol (IP) addresses constitute personal data;
- reviews the higher standards that now apply to electronic marketing as a result of both the *E-Privacy Directive* and the ASA Code;
- provides an overview of the law of privacy in an online context;
- reviews the rules on the use of location data, data retention, monitoring and surveillance.

How the cookie crumbles – an overview of data-collection technologies and techniques

4.2 Data is the currency of the internet. Collecting, analysing and selling data forms an increasingly crucial part of the business models of the world's biggest and most successful online companies. Much of this data is obtained from internet users themselves and is used for developing business strategy and sometimes, perhaps more controversially, to sell advertising. In this way, 'free' services such as search engines, email accounts and social networking sites can be financially viable business models.

The importance of data collection on the internet is shown by the multitude of technologies and methods by which data is collected from users. Such data can be divided into two broad categories: 'provided data' and 'harvested data'.

Provided data

4.3 This is data submitted directly by a user in a 'traditional' manner (eg by typing it into a website). Examples of provided data include:

- transactional data (eg credit card data and postal addresses);
- website registration details (eg email addresses and dates of birth); and
- information posted on UGC websites (eg social networking sites and blogs; see CHAPTER 6).

Harvested data

4.4 Data harvesting is a technique that builds up a profile of a user over time by aggregating information that is derived automatically from their online activities. Data harvesting relies on a method of recognising individual users as they visit websites as a consequence of the technologies by which personal computers access the internet.

At a basic level, a user can be 'remembered' when they revisit a website and perhaps receive a personalised greeting on the home page. By tracking users' activities as they move through websites, more sophisticated data harvesting can allow data collectors to analyse their users' location, language and potentially even their hobbies, interests and purchasing habits.

Several alternative technologies can be used in the process of obtaining harvested data, which are essentially different 'labels' that can be applied to individual users so that they can be recognised. Data about the user can be harvested by recording information every time the data collector sees the label (eg which web pages the user visits, when they visit them and the order they move between different web pages).

IP addresses

4.5 An Internet Protocol (IP) address is a numerical label (eg 123.234.123.234) assigned to a device that is communicating using the Internet Protocol (see CHAPTER 1). Every internet user obtains an IP address from their internet service provider ('ISP') when they connect to the internet. Every website has an IP address to which users are directed when they visit the website.

Some users' IP addresses are 'static', meaning that every time the user connects to the internet they will have the same IP address. However, most domestic internet users have a 'dynamic' IP address, meaning that their ISP assigns them a new IP address each time they connect to the internet. Dynamic IP addresses are of limited value for data harvesting. If a data collector labels a user by their IP address alone when they visit a website, the next time the user visits the website their IP address will probably be different, meaning the data collector will not recognise them and will not associate the previous harvested data with the user. Accordingly, most data collectors use IP addresses for aggregated demographic purposes (eg working out which countries provide the most visitors to their websites) rather than for profiling individual users.

4.6 *Data in a Digital World*

Cookies

4.6 Cookies were developed (in part) to resolve the shortcoming of dynamic IP addresses for user profiling. When a user visits a website that uses cookies, the website sends a cookie (a small text file that contains a unique label or 'cookie ID number') to the user's browser software and (if it is a 'persistent' cookie rather than a temporary 'session' cookie) it is stored on their computer even after they leave the website and disconnect from the internet. When the user revisits the website at a later date, their browser software returns the cookie ID number to the website, allowing the website to recognise the user and therefore to acquire further harvested data about that user. A widely used analogy is that cookies are like dry-cleaning tickets: cookies are the 'tickets' which allow websites to recognise returning users in the same way as dry-cleaning tickets allow laundrettes to return the correct clothes to each customer.

Web-bugs

4.7 Web-bugs are small, often invisible, graphics files embedded into individual web pages. These are used to track users as they move through websites. When the image is loaded, the user's browser software sends additional data to the website, such as the user's IP address, browser type and the time that the web page is visited. Web-bugs can interact with cookies on the user's computer which relate to the same website, maximising the amount of useful harvested data that can be obtained about the user. Web-bugs are also commonly used in emails to determine whether a particular user has read an email.

Webwise/Phorm

4.8 Webwise was a data harvesting system operated by the advertising technology company Phorm. Unusually, Webwise operated at ISP level (rather than at the level of individual websites) and used 'deep packet inspection' technology to enable ISPs to analyse their users' network traffic, thereby identifying keywords on every search they make and website they visit. Phorm used this harvested data to produce targeted advertising.

BT's trial of the Webwise software in 2006–7 proved controversial, not least because its users were not informed that their browsing habits were being tracked (see further PARAGRAPH 4.48 below). Several companies, including Amazon and the Wikimedia Foundation (the organisation behind Wikipedia), chose to opt out of the Webwise system and blocked Phorm from scanning visits to their websites.

The controversy surrounding Webwise focused on two issues: first, whether its unusual use of cookies complied with the *Privacy and Electronic Communications (EC Directive) Regulations 2003* (see PARAGRAPH 4.31 below); and, second, whether its surveillance of users' browsing habits was in breach of the *Regulation of Investigatory Powers Act 2000* ('*RIPA*').[1] In 2008, the Information Commissioner's Office (ICO) gave its qualified approval to the system. However, the European

[1] A detailed analysis of RIPA is beyond the scope of this book. However, a summary of the key issues in this area can be found in the European Commission's report concerning the UK's implementation of the E-Privacy Directive located at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format= HTML&aged=0&language=EN&guiLanguage=en.

Commission has since launched an investigation into whether the UK's implementation of the European legislation underlying this legislation is adequate. The Commission issued both a formal notice and a reasoned opinion but the UK failed to amend its laws in response to either. The Commission has now referred the matter to the European Court of Justice.

Combining harvested data and provided data

4.9 A powerful tool in the data collector's toolkit is to combine harvested data with provided data which the data collector already holds about the user. This can allow the data collector to 'put a face to a name' in digital terms by adding valuable harvested data to its record of an identified user.

For example, Amazon uses cookies to recognise users when they visit its website. If the user has already provided their personal details and registered an Amazon account, then the cookie ID number is automatically linked to their account. This means that Amazon knows who the user is as soon as they arrive at its website, so the user can make new purchases without providing any further personal information. Amazon also makes recommendations to users based on their previous purchases, and (by default) displays personalised third-party advertising based on certain data it holds about the user.

Targeted advertising

4.10 One of the state-of-the-art uses for harvested data is in targeted or behavioural advertising: advertising that is based on information held about the user it is directed to. This information may comprise:

- harvested information about the user's perceived interests based on their previous browsing habits; or
- (less commonly) a mixture of this harvested information and certain provided information about the user such as their age, sex, location or interests.

This process is managed by ad-serving companies (effectively an intermediary between advertisers and publishers) such as Doubleclick, and depends on cookies. When a user visits a web page that includes advertisements provided by a third party ad-server, a so-called 'third party cookie' communicates between the user's browser and the ad-serving company. The ad-serving company notes the cookie's ID number, thus learning that the user whom that cookie is labelling has viewed the web page. The web page also sends information to the ad-serving company about the contents of the web page – for example, it may be a page about sports. The resulting data (which may be owned by the ad-serving company or its advertiser client) is harvested data about the user's interests. Over time, a profile of the user is built up – if the user visits a lot of web pages about sport, the ad-serving company learns that the user is interested in sport. This takes place without any provided data being supplied by the user. Later, the user may visit another web page that includes an ad-served advertisement provided by the same ad-serving company on behalf of the same advertiser client. When the web page asks the ad-serving company for an advertisement, even if the user has never visited that particular web page before, the ad-serving company now knows that the user is interested in sports, so it is more likely to supply a sports-related

advertisement for display on the web page. Thus, the advertisement is targeted at the user based on their previous behaviour.

Provided data can be combined with harvested data in targeted advertising. If the user provides data to one website that uses targeted advertising (eg when registering with the website they may give demographic information about their age, sex and location or their interests) this data may sometimes be shared with ad-serving companies who then use it to better target advertisements on other websites. However, ad-serving companies generally avoid using information such as users' names, addresses and email addresses in targeted advertising without users' express consent.

Targeted advertising is controversial from a data protection and privacy angle, not least because users may well be unaware that they are being tracked (see PARAGRAPHS 4.16 AND 4.47 below for further analysis of the relevant law). In a study carried out by the Universities of California and Pennsylvania in September 2009,[2] 84% of respondents objected to targeted advertising when they found out it would happen by tracking them on other websites. In July 2009, a coalition of American marketing trade bodies agreed a set of seven 'Self-Regulatory Principles for Online Behavioral Advertising'[3] which included a proposal to introduce a logo to indicate when an advert was a behavioural advert. The principles will come into effect in the US in early 2011 as part of a self-regulatory programme and one of the companies, the Interactive Advertising Bureau, has since announced that it intends to roll out the use of a similar logo across the UK and EU.

Figure 1: The logo that will be used to label behavioural advertisements in the US.

(source: www.aboutads.info)

In May 2010, the Office of Fair Trading ('OFT') published the results of a market study into online targeting of advertising and prices,[4] which included an examination of behavioural advertising and customised pricing. The study particularly focused on situations where prices are individually tailored using information collected about a consumer's internet use. The OFT found that 60% of consumers would take no action at all if given the option to opt out of behavioural advertising. It recommended the development of 'clear ad' notices alongside behavioural adverts including information about opting out, and encouraged the IAB to introduce a 'one-button' opt-out tool for all its members. In addition, the OFT announced that it would establish a Memorandum of Understanding with the ICO establishing in which circumstances each party would act, should such self-regulatory measures prove insufficient.

Collection versus protection?

4.11 Data collection in the Web 2.0 world pushes the boundaries of data protection law. The increasing personalisation of websites and services, and the

2 See http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.
3 See www.bbb.org/us/Storage/0/Shared%20Documents/online-ad-principles.pdf.
4 OFT 1231.

growing reliance on sophisticated methods of targeted advertising to provide these services at no cost to their users, requires data collectors to collect and process more and more data about these users. Much of this data may be 'personal data' for the purposes of data protection legislation. But data protection laws (in Europe, at least) generally restrict data collection and processing on the basis that the less personal data is collected, the better.

Data protection rules are only relevant to 'personal data' – broadly, data which relates to an identifiable individual (see further PARAGRAPH 4.12 below). Clearly, not all data that is provided or harvested in the digital world is personal data. But, increasingly, the most useful and valuable information collected is data which does fall within this definition. As such, data protection law is now more relevant than ever to the world of digital media.

An overview of the Data Protection Act 1998

4.12 The UK *Data Protection Act 1998* ('*DPA*') (which implements *European Directive 95/46/EC* (the '*Data Directive*')) regulates the use of 'personal data' by organisations that control that data (called 'data controllers'). Personal data is data about living identifiable individuals (called 'data subjects') held either held electronically or manually as part of a 'relevant filing system'. This will generally include most data held about employees as well as certain data about customers and suppliers. Broadly, compliance with the *DPA* requires that the data controller:

- notifies an official government register of the purposes for which it is processing personal data. The regulator responsible for *DPA* compliance in the UK is the Information Commissioner and it is a criminal offence not to notify unless an exemption applies; and
- complies with the *eight data protection principles* when processing personal data. These state that personal data:
  - must be processed fairly and lawfully;
  - must not be processed for purposes incompatible with the purposes for which the data was obtained;
  - must be adequate, relevant and not excessive with respect to the purposes for which the data was collected;
  - must be accurate and, where necessary, kept up to date;
  - must not be kept any longer than is necessary for the purposes for which it was collected;
  - must be made available to individuals who request their information within 40 days of a written request and payment of a statutory fee (currently £10);
  - must be kept secure by the data controller taking appropriate technical and organisational means to prevent unauthorised processing or accidental loss or destruction; and
  - must not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection.

Application of the *DPA* to foreign companies

4.13 The *DPA* applies to a data controller if it is 'established' in the UK or if it is not established in the UK but it uses equipment in the UK for processing personal data (otherwise than for the purposes of transit through the UK). 'Established' in the UK includes maintaining an office, branch, agency or regular practice in the UK. Consequently, a foreign company with an office in the UK would be required to comply with the *DPA* as would a foreign company processing personal data on servers located in the UK.

The *DPA* provides no further indication as to the meaning of 'making use of equipment' but *recital 20* of the *Data Directive* clearly states that the law of the Member State 'in which the means used are located' should apply and the fact that the processing of data is carried out by a person established in a third country 'must not stand in the way of the protection of individuals provided for in' the *Data Directive*.

In addition, the Article 29 Working Party[5] has considered the international application of EU data protection law to personal data processing on the internet by non-EU based websites.[6] Its non-binding report suggests that making use of equipment, does not require the data controller to own or even exercise full control over the equipment and that the *Data Directive* would apply where cookies or spywares were used by a non-EU web site to collect personal data from subjects accessing sites using their PCs in the EU. We discuss cookies and spyware in more detail at PARAGRAPH 4.28 in the context of privacy.

Notification

4.14 It is a criminal offence to process personal data without notifying the Information Commissioner's Office (the 'ICO').[7] However there are some exemptions to this requirement,[8] which essentially cover processing operations involving staff administration, advertising, marketing and public relations, accounts and record keeping and certain processing operations carried out by non profit-making organisations.

Although the exemptions are quite broad, they do not permit data controllers to disclose personal data to third parties without the consent of the data subject. Consequently, they are more commonly relied upon by small to medium-sized businesses processing data solely to support their primary business activities. Larger businesses often elect to incur the small cost of notifying rather than be restricted to the limits of exempt processing, which might restrict their ability to use third party suppliers or allow third parties (even group companies) to access their databases.

The notification process is relatively straightforward and cost effective. The application form can be completed online and generally without the need for specialist advice, but must be printed off, signed and sent to the ICO with the

5 The independent EU Advisory Body on Data Protection and Privacy established by *Directive 95/46/EC, Art 29*.
6 5035/01/EN/Final WP56.
7 *DPA 1998, s 17(1)*.
8 *DPA 1998, s 17(3)*; *Data Protection* (*Notification and Notification Fees*) *Regulations 2000* (*SI 2000/188*), *Sch*.

prescribed fee, which is currently £35 (or £500 if, for example, the data controller's business has a turnover of £25.9 million and 250 or more members of staff).[9] The ICO generally processes the registration within a few days.

Even if a data controller takes the view that it is exempt from the notification requirement, it will still be required to comply with the other obligations under the *DPA*, namely the eight data protection principles.

The first principle: fair and lawful processing

4.15 'Lawful' is the more straightforward of the two concepts. Processing would be unlawful if, for example, it resulted in the committing of a criminal offence, a breach of contract or an infringement of copyright.

'Fair processing' is harder to define but generally requires that certain information is given to the data subject, usually when the data controller first processes or collects the data. This is usually achieved by way of a readily accessible privacy policy or data protection notice. The processing will not be fair unless the following information is provided (or made readily available):

- the identity of the data controller (or its nominated UK representative);
- the purpose or purposes for which the information is to be processed;
- any further information necessary to make the processing fair having regard to the circumstances.[10]

Essentially, a data controller should handle people's personal data only in the ways in which the data subject has been notified or would reasonably expect. In addition, personal data cannot be processed fairly and lawfully unless at least one of the conditions in *Sch 2* is met.

Schedule 2: Consent

4.16 The first option given at *Sch 2* is that the data subject consents to the processing.[11] There is no definition of consent in the *DPA* but the *Data Directive* provides that consent shall be 'freely given', 'specific and informed'[12] and 'unambiguously given'.[13] Consent can be express or implied.

Consent is not the only, or even necessarily the most effective, method of legitimising processing of personal data. There is, for example, some doubt in the UK and certainly in other European Member States over whether consent can be truly 'freely given' in an employment context. Certainly, Working Party guidance indicates that in an employment context reliance on consent should be confined to cases where the worker has a genuinely free choice and is subsequently able to withdraw that consent without detriment.

Notwithstanding the above, for processing of non-sensitive personal data consent is commonly achieved, not by seeking the active agreement of data subjects

9 *Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 (SI 2009/1677).*
10 *DPA 1998, Sch 1, Pt II, para 2(3).*
11 *DPA 1998, Sch 2(1).*
12 *Directive 95/46/EC, Art 2(h).*
13 *Directive 95/46/EC, Art 7(a).*

(ie signature or tick box) but by providing the data subject with sufficient information in a privacy policy/data protection notice. The ICO in its privacy notices codes of practice states that in addition to the basic legal requirements[14] to ensure that the data subject knows who the data controller is, what it intends to do with their information and who it will be shared with or disclosed to, depending on the circumstances, the data controller should also consider notifying the data subject:

- if it intends to pass information on (and the name of the organisations involved and details of how they will use the information);
- how long the data controller or other organisations intend to keep the information;
- whether the information will be transferred overseas;
- what measures are in place to ensures the security of personal data;
- about their rights and how they can exercise them – for example, the fact that a data subject can obtain a copy of their personal data or object to direct marketing;
- who to contact if the data subject wants to complain or know more about how their personal data will be used; and
- about the right to complain to the Information Commissioner if there is a problem.

However, whilst the implied/opt-out form of consent set out above (ie making a privacy notice prominently available) is currently acceptable in the UK, many European Member States favour an active opt-in approach to privacy notices, where the data subject is invited to indicate his consent by, for example, ticking a box or signing a form. See also PARAGRAPH 4.27 below in relation to the impact of the forthcoming implementation of amendments to the *E-Privacy Directive*.

Schedule 2: other options to achieve fair and lawful processing of personal data

4.17 Given the vagaries of the consent route it is not always advisable or practical for data controllers to rely solely on data subject consent to legitimise its processing. The DPA provides, in respect of the processing of personal data, several quite broad alternatives to consent, the key alternatives being that the processing is necessary:

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for the compliance of any legal obligation to which the data controller is subject;

(d) in order to protect the vital interests of the data subject; or

(e) for the purposes of legitimate interests pursued by the data controller except where it prejudices the rights and freedoms or legitimate interests of the data subject.[15]

[14] *DPA 1998, Sch 1, Pt II, para 2(3).*
[15] *DPA 1998, Sch 2, paras 2, 3, 4* and *6.*

Sensitive data

4.18 Sensitive personal data means personal data consisting of information as to:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- whether the data subject is a member of a trade union;
- physical mental health/condition;
- sexual life;
- commission or alleged commission by the data subject of an offence; or
- any proceedings for any offence committed or alleged to have been committed by the data subject.[16]

Sensitive personal data cannot be processed fairly unless one of the conditions in *Sch 3* is met.

The first option provided in *Sch 3* is that processing of sensitive personal data may be fair if 'the data subject has given his explicit consent to the processing of the personal data'. The ICO has stated that explicit consent should be absolutely clear, cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made. The standard UK approach for complying with this requirement is to provide a comprehensive notice together with an opt-in box to indicate positive prior consent. The ICO has also made specific comments in relation to employee consent, namely:

- the worker must have been told clearly what personal data is involved and have been properly informed of the use that will be made of it. The worker must have given a positive indication of agreement (eg a signature); and
- the consent must be freely given. This means the worker must have a real choice whether or not to consent and there must be no penalty imposed for refusing to give consent.[17]

The opt-in approach outlined above is the one adopted generally across Europe, but there are some notable exceptions, with certain Member States requiring the written consent of the data subject. In addition, certain European countries expressly prohibit the processing of sensitive personal data about racial or ethnic origin in the context of employment.

The alternatives to consent are far narrower than those provided for non-sensitive personal data. For example, processing can be fair if it is necessary in order to protect the vital interests of the data subject but only where consent cannot reasonably be obtained or has been unreasonably withheld (ie life or death situations). There are further public interest/security exceptions set out in the *Data Protection* (*Processing of Sensitive Personal Data*) *Order 2000*, but these are of little

[16] *DPA 1998, s 2.*
[17] Supplementary Guidance to the ICO's 'Employment Practices Data Protection Code'.

relevance to most businesses. In most cases the explicit consent of the data subject will need be obtained prior to the processing of sensitive personal data.

Rights of data subjects: Direct marketing

4.19 The *DPA* provides that the data subject is entitled at any time by notice in writing to require the data controller to stop processing his personal data for the purposes of direct marketing (that is marketing which is specifically addressed to an individual).[18] In other words the data subject must be provided with the opportunity to opt-out of such communications. In addition, there are specific rules that relate to direct marketing by email which were implemented under the UK regulations[19] which gave effect to the *E-Privacy Directive*.[20] Under the regulations it would seem that individuals must actively agree to receiving marketing by electronic mail (ie opt-in consent is required) although certain exceptions apply. This is covered in more detail at PARAGRAPHS 4.31–4.32.

Rights of data subjects: Access requests

4.20 Subject to certain exemptions, where a data subject makes a request in writing (including by email) and pays the appropriate fee (maximum £10), he is entitled to be informed if a data controller (or a data processor) is processing data of which he is a subject and if so, to be given a description of:

- the personal data;
- the purposes for which they are being processed;
- those to whom they are or may be disclosed;
- any information as to the source of the personal data; and
- in the situation where automated decision making takes place, there are certain other rights to information. [21]

In addition, the data subject is entitled to an (electronic or hard) copy of such personal data. The data subject is not necessarily entitled to copies of original documents; it is the information constituting the personal data contained in the document that must be supplied in an intelligible and permanent form. It is therefore permissible to create a new document which sets out the information which constitutes personal data particularly if, for example, the original document contains third party personal data or includes irrelevant information.

The data controller must supply the information promptly and in any case within 40 days of having received the request.[22] However, it is possible to delay responding if:

- the data subject has not sent the prescribed fee;
- further information is required to verify the data subject's identity (but this may be obvious from the postal address and signature); or

18 *DPA 1998, s 11.*
19 *The Privacy and Electronic Communications (EC Directive) Regulations 2003.*
20 *EC Directive on Privacy and Electronic Communications (2002/58/EC).*
21 *DPA 1998, s 7(1).*
22 *DPA 1998, s 7(8).*

- more time is needed to locate the information which the data subject seeks (the more specific the request is, the less likely this is to apply).[23]

The data controller would then be required to reply within 40 days of receipt of the prescribed fee or the further information.

Rights of data subjects: Preventing processing

4.21 *Section 10* provides that a data subject can, by providing notice in writing, require a data controller to 'cease' processing for a specified purpose or in a specified manner, if:

- it is likely to cause substantial damage or substantial distress; and
- that damage or distress would be unwarranted.

A data subject can seek a court order if he considers that the data controller has not complied with his *s 10* notice.

The data subject also has a right at any time by notice in writing to the data controller to prevent processing that is causing or likely to cause unwarranted damage to him or another; and an unqualified right to prevent processing for the purposes of direct marketing.[24]

Section 14 relates to 'rectification, blocking, erasure and destruction' of inaccurate data and cannot be enforced directly by a data subject but only on application to the court/court order.

Data processing agreements

4.22 A data processor means any person who processes personal data on behalf of a data controller. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must, in order to comply with its security obligations under the *DPA*:

- choose a data processor providing sufficient guarantees in respect of technical and organisational security measures; and
- take reasonable steps to ensure compliance with those measures.[25]

The processing must also be carried out under a written contract which states that the data processor:

- is to act only on instructions from the data controller; and
- is required to comply with obligations equivalent to those imposed on the data controller by the seventh principle.[26]

Liability for data processing under the *DPA* remains with the data controller so it is important that the data processing agreement imposes adequate contractual obligations on the data processor. However, if a data processor exceeds or disregards the instructions of the data controller it is likely to be in breach of

[23] *DPA 1998, s 7(3).*
[24] *DPA 1998, ss 10 and 11.*
[25] *DPA 1998, Sch 1, Pt II, para 11.*
[26] *DPA 1998, Sch 1, Pt II, para 12.*

contract and it may find that it is liable as a data controller by virtue of the independence it has exercised in respect of that personal data.

Sub-processing agreements

4.23 Increasingly data processors will sub-contract some element of their services and the data processing services to one or sub-contractor (ie appoint a sub-processor). The appointment of sub-processors, whilst commercially common, is not something mentioned or even envisaged under the *DPA* or the *Data Directive*. Notwithstanding this, a data controller can be liable for any acts of its sub-processors, even though there may be no privity of contract between them.

Consequently, where sub-processing is likely it is important to deal with it in the data processing agreement so that it is possible to demonstrate a contractual chain of liability. We would recommend including in the data processing agreement clauses which provide that the data processor can only appoint a sub-processor by way of a written agreement which:

- imposes the same obligations on the sub-processor as are imposed on the data processor under the data processing agreement; and
- provides at least the same level of protection for the personal data and the rights of data subjects as exist under the data processing agreement.

The future direction?

4.24 In November 2010, the European Commission announced[27] that it intends to propose in 2011 a new general legal framework for data protection in the EU. It is intended that this will strengthen and harmonise data protection laws across the EU, and bring existing laws up to date with 'the challenges raised by new technologies and globalisation'. Among the initial proposals is that:

- users should know and understand about how their internet use is being monitored for the purposes of behavioural advertising. For example, people should be aware when online retailers use previously viewed web sites as a basis to make product suggestions.
- there should be a 'right to be forgotten,' which means that individuals should have the right to have their data fully removed when it is no longer needed for the purposes for which it was collected.

The Commission stated that it will also 'consider and pursue non-legislative measures, such as promoting awareness-raising campaigns on data protection, encouraging self-regulation and the possibility of EU certification schemes in the field of privacy and data protection.'

Though details are few and far between at the date of writing, it is likely that such an updated legal framework would tackle many of the ambiguities of data protection in a digital world head on. However, any new legislation introduced would probably take several years to be implemented and come into force in Member States.

[27] Commission Press Release IP/10/1462

Personal data in a digital world

4.25 As the above summary shows, data protection laws regulate the use of personal data. However, not all data that is harvested or provided online is personal data – and data that is not personal data falls outside the scope of the *DPA*. Drawing the line between what is and is not personal data is therefore an important distinction for data collectors to understand.

Personal data is defined in the *DPA 1998, s 1*(*1*) as:

> '… data which relates to a living individual who can be identified—
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.'

It is important to note that this definition does not require knowledge of the individual's name. As the Article 29 Working Party notes:

> '… while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other 'identifiers' are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the person registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact.'[28]

Harvested data

4.26 In respect of harvested data, there are two separate issues to address – whether the 'labels' used to recognise users when collecting harvested data (IP addresses and cookies) can be regarded as personal data, and whether the harvested data itself falls under this definition.

IP addresses

4.27 An IP address in itself contains a limited amount of freely available information. IP addresses are typically assigned to ISPs in batches, which means that a user's choice of ISP and some geographical data (but typically only down to a city or region) can generally be derived from their IP address.

[28] Article 29 Working Pty Opinion 4/2007 on the concept of personal data (20 June 2007) at p 14.

The ICO draws a distinction between static and dynamic IP addresses. As dynamic IP addresses change each time a user connects to their ISP, the ICO suggests that 'if it is only the ISP who can link the IP address to an individual it is difficult to see how the [*DPA*] can cover collecting dynamic IP addresses without any other identifying or distinguishing information'.[29] Further, since 'it is not easy to distinguish between dynamic and static IP addresses', the ICO considers that there is limited scope to use static IP addresses for personalised profiling either (see further PARAGRAPH 4.29 below).

The Article 29 Working Party has a more restrictive approach which states that unless a data collector (be they an ISP or a website operator) can be absolutely certain that a user cannot be identified from their IP address, 'it will have to treat all IP information as personal data, to be on the safe side'.[30]

Google's view is that IP addresses should not be categorised in 'black-and-white' as always being personal data because this:

> '… incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you're an ISP and you assign an IP address to a computer that connects under a particular subscriber's account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings.'[31]

This argument implies that whether an IP address is personal data depends on whose hands it is in. If a data collector can connect an IP address with other personal information it holds about the user of that IP address, the IP address becomes personal data, because it then falls within the *DPA* definition (ie it relates to an individual who can be identified from the data and other information which is in the possession of the data collector). Google's argument is that whilst an ISP is in a position to make that connection as it maintains records of which dynamic IP addresses are assigned to which users, other websites cannot usually do this as they do not maintain such records.

Cookies

4.28 Generally, cookie files do not contain any personally identifiable information and as such cookies in themselves are unlikely to fall within the definition of personal data. However, unlike dynamic IP addresses, (persistent) cookies are lasting labels that continue to attach to users over multiple internet sessions. Therefore, if a data collector connects harvested data obtained through the use of cookies with other personal data it holds about the user (eg provided data about the user's contact details), the ICO's view is that this harvested data will also become personal data – meaning that data collectors must comply with the *DPA* requirements in relation to such data:

[29] ICO Data Protection Good Practice Note – Collecting personal information using websites (v2.0, 5 June 2007) at p 3.
[30] Article 29 Working Pty Opinion 4/2007 on the concept of personal data (20 June 2007) at p 17.
[31] Google Public Policy Blog: Are IP addresses personal? (22 February 2008).

> 'Website operators using cookies are able to track the online movements of an individual and may be used to develop a profile of them. If the operator intends to link this profile to a name and postal address, or an email address, this is personal information covered by the [*DPA*]. However, operators can develop and use profiles by using cookies without collecting traditional identifiers. Our view is that, in the context of the online world, the information that identifies an individual is that which uniquely locates them in the world, by distinguishing them from others. So, profiles based on the information collected by cookies which are linked to other information which uniquely identifies the individual are personal information and covered by the [*DPA*].'[32]

Data collectors must also comply with several further legal requirements in relation to the use of cookies. (Note that where cookies are used in connection with processing personal data, the data collector must comply with both the *DPA and* these further requirements.) The extra regulations for cookies derive from the *E-Privacy Directive, Art 5*(*3*).[33] This states that the use of technology such as cookies is permitted, provided that the user is:

- given 'clear and comprehensive information' about the purposes of the use of the technology; and
- offered 'the right to refuse' (ie opt out of) the use of the technology.

Exceptions from these requirements apply where:

- the sole purpose is to facilitate electronic communication; or
- the use of the technology is strictly necessary to provide a service explicitly requested by the user.

These provisions were implemented in virtually identical form in the UK by *E-Privacy Regulations, reg 6*.[34] However, *reg 6*(*3*) makes it clear that if cookies are used by the same data collector to store or access information from the same user on more than one occasion, it is sufficient for the above conditions to be met in respect of the initial use.

In the UK, it is currently considered sufficient to include the information on cookies and details of how to opt out in a privacy policy, for example:

> '[Website] makes use of cookies which are files placed on your computer that enable us to track certain information relating to your use of [Website]. Cookies allow us to better customise your visit to individual preferences helping us to provide you with the best possible service on [Website]. We use cookies to (1) simplify the logging on process; (2) ensure the security and authenticity of users; (3) provide mechanisms for online shopping; and (4) enable traffic monitoring. You may be able to configure your web browser to prevent the use of cookies although some functions or services may not then be available. For more information on the use of cookies and how to disable them, we recommend www.allaboutcookies.org.'

[32] ICO Data Protection Good Practice Note – Collecting personal information using websites (v2.0, 5 June 2007) at p 2.
[33] See PARA 4.31 below.
[34] Ibid.

However, the position will be changed by an amendment to the *E-Privacy Directive, Art 5(3)* which was introduced by a new Directive (*2009/136/EC*). Member States must implement it by 25 May 2011. The amendment replaces the requirement for a right to opt out with a requirement that the user has given their *consent*. Before giving such consent, the user must first (as before) have been provided with 'clear and comprehensive information' about the purposes of the use of the technology. The same exceptions will apply with minimal amendments.

It is presently unclear whether this amendment will introduce an 'opt-in' regime across the EU where prior explicit consent to the use of cookies will be required. There is currently no binding guidance to the new rules, although *Recital 66* to the amending Directive say that 'where it is technically possible and effective …consent to processing may be expressed by using the appropriate settings of a browser'. Arguably, this suggests that something less than explicit consent may be required. The Recitals also state that 'the methods of providing information and offering the right to refuse should be as user-friendly as possible' and call for enhanced powers to be granted to national authorities so that they may enforce these requirements more effectively.

In June 2010, the Article 29 Working Party issued an opinion[35] which concluded that to comply with the amended *E-Privacy Directive*, users will be required to specifically opt in to cookie use; that is, on each visit to a website, pop up boxes should be displayed on entry to the site informing the user about the use of cookies on that site and asking users to positively agree to their use.

In respect of the caveat in *Recital 66* to the amending Directive, the Article 29 Working Party's view is that browser settings should only deliver consent in very limited circumstances. This, it said, is because the current default on most browser settings is to accept cookies and many users would simply not bother (or not know how) to change that. In its view, browser settings should only deliver consent to cookie use where the browser was set up by default to reject cookies. This would mean that users would have to change the setting affirmatively to accept cookies (in other words, specifically opt in).

Although the opinion is not legally binding, it has caused concern amongst website operators and online advertising providers because of the potential costs of complying with a strict opt-in regime and, more significantly, the likely disruption to the user experience which could result in loss of customers.

However, following the publication of the Article 29 Working Party opinion, in September 2010 the UK government launched a consultation[36] on the implementation of the amended *Article 5(3)* into UK law. Interestingly, in its impact assessment to accompany the consultation, the government rejected creating an opt-in regime for cookie use generally, stating its view that such a regime would require users to consent to every cookie placed on their computer and this would lead to a permanent disruption of online services and to online providers suffering substantial losses. Instead, it proposed simply to copy the amended *Article 5(3)* verbatim into UK law and leave it to the ICO to specify what website operators/

[35] http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_06_10_en.pdf
[36] http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10–1133-implementing-revised-electronic-communications-framework-impact.pdf

online advertisers are required to do in terms of obtaining consent to cookies, saying this would allow greater flexibility to keep track with changes in technology and usage.

The government's impact assessment also proposed to allow online providers to take advantage of *Recital 66*; that is, users would be allowed to demonstrate consent to cookies simply by their browser setting being set to accept them. However, the government's view was that users should be given clear and comprehensive information about cookie use and how to opt out if they wish. They should also be given information about using browser settings for this purpose, including how to alter settings to accept or reject cookies as required. The government declined to give guidance on when cookie use will be '*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*' saying that, given the fast paced nature of the internet, it would be almost impossible to do this without risking damaging innovation.

Unless this changes following the consultation, it seems that the current position on cookie use will remain largely unchanged; that is, users must be given information about cookie use and how to opt-out (using browser settings) but no opt-in consent regime will be introduced. This will, however, be in direct conflict with the Article 29 Working Party's opinion.

Concerns have also been raised about the 'Flash cookie', a more recent form of cookie which is stored separately from normal (http) cookies on computers and which remains largely undetected by web browser privacy settings. A survey carried out by researchers at the University of California, Berkeley[37] showed that Flash cookies were used by 54 of 100 leading websites, but that they were mentioned in the privacy policies of only four of these websites. Some websites even used Flash cookies to 'respawn' (recreate) http cookies that had been deleted by the user. It is dubious whether such practices would comply with the *E-Privacy Regulations*, particularly if the user is unaware of them.

Provided data

4.29 Provided data is only personal data if it fulfils the requirements of the *DPA* definition itself or when it is connected to other personally identifiable information. This means that if a data collector holds provided data from which it is unable to identify an individual either from the data itself or in combination with other data it holds, the use of such provided data falls outside the *DPA*.

This is central to the targeted advertising strategies of companies such as Facebook and Google. Although advertisers may choose who they wish to target, no personally identifiable data is passed back to the advertisers. Rather, advertisers will only see aggregated and non-specific information (eg the number of times their advertising has been viewed). Hence – the argument goes – as no personal data is shared with a third party, no *DPA* issues will arise.

Conversely, the *DPA* applies where provided data that *is* personal data is passed to third parties. The ICO has issued guidance in relation to such a situation:

[37] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

> 'If you get information from a third party, for example, directly from another website operator or harvested from a website, you still have a duty to make sure any subsequent processing of the information is fair. This may involve making sure that the individual knows that you hold their information and what you are using it for.'[38]

When should the individual be informed? Sometimes, the ICO says, it may be possible to inform the individual before their information is collected from the third party. In other cases, the third party may have already informed the individual. If not, the data collector should provide the requisite information to the individual '*as soon as possible after obtaining their personal information.*' An exception from the requirement to contact the individual applies where this would involve 'disproportionate effort', but the ICO's view is that this only applies in very limited circumstances. If the data collector decides the exception does apply, the information must still be provided to any individual who requests it, and the data collector must keep a record of the reasons for its decision.[39]

This has ramifications for both provided and harvested data:

- where the data is shared with third parties, the parties sharing the data should agree who will inform the user of this – preferably this should occur before the data is shared (eg by making clear reference to such practices in the privacy policy of the website which originally received the data).
- where harvested data is collected by or passed to third-party ad-serving companies, the parties should ensure that the user is aware of this practice.

Additional rules apply to contact details such as telephone numbers and email addresses which users may provide to data collectors – see PARAGRAPHS 4.32 AND 4.33.

The future of personal data?

4.30 In October 2010, the ICO published a statement[40] calling for a clarification of the definition of personal data, particularly online, and suggesting that using information from IP logs to identify individuals (eg for targeted advertising) should attract some (appropriate) form of data protection:

> 'There is a lack of clarity in the current data protection legislative framework in the UK in determining what is 'personal data'. This arises in part because the wording of the UK *DPA* is different to that in the EU [Data Directive]. Whilst both definitions can be interpreted as meaning essentially the same thing, case law and the advances in technology have led to confusion about what the definitions mean in practice, and the data that comes within their scope. Any revision of the current legislative framework should be seen as an opportunity to remove this area of doubt and provide data controllers with greater legal certainty as to what constitutes personal data.

38 ICO Data Protection Good Practice Note – Collecting personal information using websites (v2.0, 5 June 2007) at p 4.

39 See *Data Protection* (*Conditions under Para 3 of Pt II of Sch I*) *Order 2000* (*SI 2000/185*), *arts 4* and *5*.

40 http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/response_to_moj_dpframework.ashx

> In the Commissioner's opinion, a future framework must deal better with the new forms of identification that are coming into being all the time, particularly in the online environment. It is clear that information such as IP logs held by search engines are being used to identify individuals and to take action affecting them, in contexts ranging from behavioural advertising to digital rights management or national security. It is clear that data protection ought to apply to this sort of information. However, we have to be realistic about how such information is treated under the law, what standards we expect those processing it to reach and what outcomes we are seeking for the individual. Whilst we may want this information to be kept secure and protected from inappropriate disclosure, it may be impossible in practice to grant conventional subject access to it or to expect individuals to consent to its processing. The Commissioner hopes that a future framework will treat this sort of information more realistically, perhaps recognising that a simple 'all or nothing' approach to the application of data protection requirements no longer suffices, given the breadth of information now falling within the definition of personal data.'

It is conceivable that such a development could form part of the EU-wide new general legal framework referred to in PARAGRAPH 4.24 above.

The E-Privacy Regulations

4.31 The *Privacy and Electronic Communications* (*EC Directive*) *Regulations 2003* (the '*E-Privacy Regulations*') implement in the UK the requirements of the *EC Directive on Privacy and Electronic Communications* (*2002/58/EC*) (the '*E-Privacy Directive*') and, amongst other things, regulate telephone marketing and marketing by unsolicited electronic mail.

Regulation 4 makes clear that the *E-Privacy Regulations* are supplemental to, and do not replace, the requirements of the *DPA* in respect of such communications. This means that there is a higher standard imposed on data collectors who use provided data for such activities.

Telephone marketing

4.32 The *E-Privacy Regulations* impose a number of restrictions on telephone marketers. In particular:

- *Regulation 19* prohibits the use of automated calling systems (systems which automatically initiate a sequence of calls to more than one destination and transmit recorded messages to recipients) for direct marketing purposes without the prior consent of the recipient of the call; and
- *Regulation 21* prohibits unsolicited calls for direct marketing purposes where the recipient has asked the caller not to receive such calls or has registered with the Telephone Preference Service. *Regulation 20* sets out similar restrictions on direct marketing by fax.

Electronic direct marketing

4.33 *Regulation 22* significantly restricts direct marketing by electronic means, by prohibiting the sending of unsolicited communications by electronic mail for direct marketing purposes, unless the recipient has given his prior consent or the soft opt-in exception applies (see below).

'Electronic mail' in this context means any message directed to particular individuals or companies consisting of text, voice, sounds or images. Hence, this prohibition includes email but also text, picture and video messages, answer phone and voicemail messages.

The ICO's definition of consent is 'some form of communication where the individual knowingly indicates consent'. Essentially, this means the explicit consent of the recipient.

This requirement to obtain consent to emails and other electronic communications is commonly achieved by means of tick boxes on website registration forms. For instance, to register on eBay.co.uk, the user must tick a box to confirm their agreement that: 'I may receive communications from eBay and I understand that I can change my notification preferences at any time in My eBay.'

Additionally, *Regulation 23* requires that in any direct marketing communications by electronic mail:

- the sender's (ie the data collector's) identity must not be disguised or concealed; and
- a valid contact address for the data collector to be given so that the recipient can opt out of future communications must be included.

Soft opt-in

4.34 *Regulation 22*(3) contains a limited exception from the general requirement for data collectors to obtain explicit consent from the recipient to engage in electronic direct marketing, where the following three conditions are all met:

- the data collector has obtained the recipient's contact details in the course of a sale or negotiations for the sale of a product or service to that recipient;
- the direct marketing material the sender is sending relates to the data collector's similar products and services only; and
- the recipient was given a simple means of opting-out, free of charge except the cost of transmission (eg a standard SMS, tick-box, email or website link) at the time their details were initially collected and also at each subsequent communication.

The ICO has issued guidance on its interpretation of the *E-Privacy Regulations* and the soft opt-in exception in particular. In the ICO's view, the requirement to obtain details 'in the course of a sale or negotiations for a sale' does not require that the sale was completed. Rather, it is sufficient that 'a person has actively expressed an interest in purchasing a company's products and services' and not opted out of further marketing of that product or service or similar ones.

The ICO takes a purposive approach to the definition of 'similar products or services', stating that 'the intention is to make sure an individual does not receive promotional material about products or services that they would not reasonably expect to receive'. This does not preclude marketing by companies affiliated with the original sender.

The ICO has stated that details obtained as part of a competition (to raise interest in a product or service) may constitute negotiations if the reason for collection was clear at the time. However, the use of cookie technology to identify a person's interests while browsing a website does not constitute negotiations. The soft opt-in exception does not apply to lists of recipients bought in externally, or to viral advertising (as to which see CHAPTER 5). In each case, the explicit consent of the recipient to receive the communication is required.

Ultimately, if recipients are unhappy at receiving communications sent by data collectors by virtue of the soft opt-in exception, they can opt out of receiving future communications. The ICO has stated that marketers must act on and respect opt-outs, and indicated that it will focus particular attention on failures to comply.

Other jurisdictions

4.35 *The E-Privacy Directive* is interpreted more strictly in other European jurisdictions. In France, consent is subject to a strict opt-in regime, and direct marketing may not be sent via email unless the sender has the prior consent of the recipient.

In Germany, the laws on direct marketing by post have recently been amended. An organisation must have a consumer's permission to use their address unless:

- they have an existing relationship; or
- the sender names the source of the address on the direct mail envelope.

Furthermore, 'unfair competition' laws – which do not exist in the UK – prohibit unwanted advertisements and further restrict the use of provided data in France, Germany and other European jurisdictions.

CAP Code rules

4.36 As noted in CHAPTER 5 the Committee of Advertising Practice ('CAP') is the self-regulatory body for all non-broadcast advertising. It is responsible for the British Code of Advertising, Sales Promotion and Direct Marketing ('the CAP Code'), which covers non-broadcast marketing communications across a range of media, and extends to email, text messages and the internet (including banners, pop-ups, virals and sponsored searches).

The CAP Code echoes and reinforces the provisions of the *E-Privacy Regulations* relating to unsolicited electronic marketing communications. *Rule 43.4*(*c*) states:

> 'The explicit consent of consumers is required before …[sending] marketing communications by email or to mobile devices, save that marketers may send unsolicited marketing about their similar products to those whose details they have obtained in the course of, or in negotiations for, a sale.

> They should, however, tell them they may opt-out of future marketing both when they collect the data and on each occasion they send out marketing communications and should give them a simple means to do so. Explicit consent is not required when marketing business products to corporate subscribers, including to their named employees.'

Rule 22.1 also requires that 'unsolicited email marketing communications should be clearly identifiable as marketing communications without the need to open them.'

The Advertising Standards Agency ('the ASA') has reprimanded several advertisers for failure to comply with the CAP Code regarding unsolicited direct marketing.[41]

The eighth principle and cross-border data flows

4.37 The Eighth data protection principle provides that:

> 'Personal data shall not be transferred to a country or territory outside the European Economic Area ('EEA')[42] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

Transfer of personal data is not defined in the *DPA* or the Data Directive. It would typically be understood to mean the sending or transmitting of personal data from one place to another. ICO guidance provides that transfer does not mean the same thing as mere transit and the fact that personal data may be routed through a third country does not mean that it is a transfer for the purposes of the eighth principle.[43]

The concept of mere transit should be construed narrowly; European Commission guidance provides that 'all the cases where a data controller takes action to make personal data available to a third party located in a third country' could fall foul of the eighth principle. This would not include a data controller in the EU making personal data available in a third country on an internet page provided that the hosting is also provided in the EU,[44] but the application of the eighth data protection principle should be carefully considered if hosting (or other technical support) is to be provided from outside the EU.

Which countries outside the EEA ensure an adequate level of protection?

4.38 The European Commission has the power to determine which countries outside the EEA have 'an adequate level of protection'. The Europa website

[41] For a rather unusual example of an email advertisement that was held to breach both *rr 22.1* and *43.4(c)*, see the ASA Adjudication on *Metrodome Group plc* (6 May 2009), concerning an email which led recipients to believe that they were under criminal investigation for drugs offences. In fact, the email was a promotion for the British film 'Shifty'.

[42] The EEA consists of the EU Member States together with Iceland, Liechtenstein and Norway.

[43] Paragraph 1.3.2, The eighth data protection principle and international data transfers, v3.0, 17.12.08.

[44] See Case C-101–01, *Bodil Lindqvist*, ECR, 2003- P I-12971.

contains an up-to-date list which currently includes Switzerland, Canada (subject to conditions), Argentina, Guernsey, Jersey, the Isle of Man, Faroe Islands, Israel and Uruguay.

In addition, the European Commission has approved the US Department of Commerce's Safe Harbor Privacy Principles, under which personal data can be transferred to US organisations who have agreed to comply with a set of standards broadly equivalent to the *Data Directive*. Approximately 1,700 US companies (including many major multi-nationals) are safe-harbor certified. The procedure involves a self-certification regime and requires the US organisation to implement an internal privacy programme to certify that it meets EU data protection standards; it can then re-certify annually by performing a self-assessment to verify its compliance with the principles.

If the personal data is not being transferred to a country deemed 'adequate' or a US company that is safe harbor registered, it is possible for the data controller/exporter to determine adequacy itself having regard to all the circumstances of the case and the factors set out in *DPA 1998, Sch 1, Part II, para 13*. However, as the assessment is subjective it is preferable not to rely solely on self-assessment and to also have in place one of the other safeguards provided for in *DPA 1998, Sch 4* unless the nature of data being transferred is particularly low risk (ie the risk that the data subject would suffer significant damage if adequate protections were not in place is low).

Exceptions to the prohibition on transfers

4.39 For the purposes of most businesses, the key exceptions to the eighth principle prohibition are:

- the data subject has given consent;
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the transfer is necessary for the conclusion or performance of a contract between the data controller and a person other than the data subject, but which is entered into at the request of the data subject, or is in the vital interests of the data subject; or
- the transfer has been made on terms which are of a kind approved by the ICO (ie contractually or under binding corporate rules).[45]

Consent

4.40 In the UK, data controllers frequently obtain consent by providing the data subject with access to clear notices (usually contained in a privacy policy) prior to collecting the data. The ICO guidance provides that such a notice should specify the reasons for transfer and, as far as possible, the countries involved, as well as any particular risks involved.[46] A consent clause that is drafted too broadly risks being invalid.

[45] *DPA 1998, Sch 4 paras 1,2, 3* and *8*.
[46] ICO, Data Protection Guidelines, International Transfers of Personal Information, v3.0, 30/10/08.

European Commission guidance on this subject (though non-binding) clearly sets out that 'consent must be a clear and unambiguous indication' of the data subject's wishes and that this 'is likely to mean that many situations where consent is implied (eg because an individual has been made aware of a transfer and has not objected) would not qualify' for this exception.[47] It also points out that where consent is sought in an employment context 'the employee must have a real opportunity to withhold his consent without suffering any harm' and the Article 29 Working Party recommends that employers should not rely solely on employee consent when transferring data.

In addition, consent is very unlikely to be practical where the data has already been collected (eg where a company is restructuring or outsourcing part of its operations to a third country it is unlikely to want to provide notice to each of its customers and employees).

Performance of the contract

4.41 To rely on this exception, the data controller has to demonstrate that the transfer is genuinely necessary for the performance of the contract. This would usually apply if the data controller were providing service or order fulfilment at the data subject's request (eg a customer ordering a product from a retailer in the UK, the retailer providing the customer's name and address to a manufacturer/supplier in the US for shipping) but it is unlikely to be effective simply because of the way a business is structured (eg an international group of companies which chooses to process its payroll centrally and outside of the EU).

Contracts approved by the ICO

4.42 Personal data can be transferred outside of the EEA where a contract ensuring adequate safeguards for the rights and freedoms of data subjects is in place. These contracts can be based on the standard contractual clauses approved by the European Commission (known as the model form contracts) and in the UK such contracts can be in a bespoke form.

Standard contractual clauses or model contracts are contractual terms that have been approved by the European Commission and the ICO. There are two sets of model contracts: controller-to-controller transfers and controller-to-processor transfers. Whilst a data controller will need to insert certain information into the model contracts (eg names of the parties, security measures, governing law), the data controller must not make any amendments to the terms or the contract will no longer (automatically) be deemed to provide an adequate level of protection.

Model contracts have been criticised as being long and unduly onerous. In particular, parties are often reluctant to accept the provisions allowing data subjects to seek compensation from data exporters and (if it is not possible to enforce against the exporter) to enforce against the data importer. However, they are the only form of contracts which can be used Europe wide and which provide legal certainty in relation to transfers.

[47] Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries.

Bespoke contracts should only be used in respect of data transfers solely from the UK but as the ICO is not able to give detailed advice or approve contracts other than in exceptional circumstances bespoke contracts are likely to be too legally uncertain for transfers of sensitive or high risk personal data.

Binding corporate rules are essentially a stringent form of intra-group privacy policy, which can be approved by the ICO. Currently, GE, Philips, Accenture, Atmel and the Hyatt Hotel Corporation are the only companies to have obtained authorisation.

Issues around specific US/EU conflicts of law

4.43 A tension exists between disclosure obligations under US regulatory rules and the application of the EU data protection requirements; the tension is not so acute in the UK due to the manner in which the UK has implemented and interprets its data protection obligations, but in other European Member States these contradictory requirements can be actively incompatible. In many ways the divide is cultural, with European suspicion of centrally held personal data arguably a reaction to the control and manipulation of personal data that occurred in many Member States under fascism.

Equal opportunities monitoring

4.44 In the US many companies are required to file a report, for the purposes of equal opportunities monitoring, which provides statistical data on the race, ethnicity and gender of its employees and job applicants. In the UK the *DPA* specifically states that processing of sensitive personal data relating to racial or ethnic origin can be fair in the context of equal opportunity monitoring,[48] but in other European Member States the collection of such data in the context of employment is never acceptable even if express consent is sought. In such circumstances, a US company with a presence in Europe is required to process such data, and will have to ensure that no processing of that data occurs in the EU (ie that the *Data Directive* does not apply). In other words, the data should only be requested for US jobs and only accessed (and ideally stored) in the US.

Even if such measures are taken, this remains something of a grey area as the Directive provides that local data protection law will apply if the data controller 'makes use of equipment'[49] in the territory (eg it is possible that a US company could be subject to French data protection law simply because a data subject in France enters race/ ethnic origin information in respect of a US job). The Article 29 Working Party is of the opinion that this would not be sufficient to constitute processing in the EU, but this has not been confirmed by a decision of the European Court of Justice.[50]

The Sarbanes-Oxley Act 2002

4.45 The Sarbanes-Oxley Act 2002 (SOX) requires publicly held US companies to provide a confidential and anonymous mechanism for its employees to report

[48] *DPA 1998, Sch 3, para 9.*
[49] *Art 4(1)(c).*
[50] The opinion of the Working Party (5035/01/EN/Final).

questionable accounting or auditing matters. By contrast, whistle blowing, in particular anonymous whistle blowing, remains controversial in Europe as it is uncertain whether collecting/storing/investigating a claim made by a whistle-blower against another individual (a 'data subject') without that person's knowledge or consent satisfies the first data protection principle (ie that 'personal data shall be processed fairly and lawfully').

There is no prohibition on anonymous whistle blowing in the UK, but in many European Member States anonymous hotlines are not permitted, or are only permitted in exceptional circumstances.

As yet the ECJ has not ruled on this issue, but the Article 29 Working Party has published an opinion on this matter. The Working Party considered that a whistle blowing policy can be lawful if it is 'necessary for the purposes of a legitimate interest pursued by the controller' but that 'such a reason would only be acceptable on the condition that such legitimate interests are not overridden by the interests for fundamental rights and freedoms of the data subject', in other words the data subject's rights must be adequately protected.[51]

Enforcement

4.46 The government has recently enacted legislation which gives the ICO greater enforcement powers. Since 6 April 2010 the ICO has been able to impose fines of up to £500,000 for breaches of the data protection principles. The breach must be:

- serious and likely to cause substantial damage or distress;
- deliberate; or
- done with knowledge of the risk of a breach and the fact that substantial damage or distress would be caused and no reasonable steps were taken to prevent it.[52]

The ICO sets the level of the fine and guidance suggests a higher fine will be imposed where an organisation cannot show that it has adequate data management procedures in place. The new powers only apply to contraventions occurring on or after 6 April 2010.

For less serious offences, the ICO's enforcement powers remain relatively weak. The Commissioner can bring proceedings in relation to certain offences such as processing without registration/failure to notify and *section 55* offences relating to unauthorised access to and disclosure of personal data,[53] but for most breaches of the data protection principles the Commissioner must first issue an enforcement notice,[54] which essentially sets out the breach and requires its remedy. It is only

[51] WP 117 Opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

[52] Information Commissioner's guidance about the issue of monetary penalties prepared and issued under *DPA 1998, s 55C(1)*, 12 January 2010.

[53] *DPA 1998, s 60.*

[54] *DPA 1998, s 40.*

when that enforcement notice is breached that an offence is committed and prosecution is possible.[55] The fine for such offences is limited to the statutory maximum of £5,000.

Use of location data

4.47 A recent raft of online applications such as Loopt, FourSquare and Fire Eagle now allow users to download information relevant to their current geographical location and to post information about their whereabouts onto UGC sites. These applications, whose popularity is booming with the growth of internet-enabled portable devices such as mobile phones, tablet computers and netbooks, use location data to pinpoint a user's location and transmit it back to the data collector, where it can be used to plot the user's position either individually or relative to other physical objects, places or other users. This can then be used to supply relevant local content to the user.

For instance, the Canadian newspaper Metro announced in January 2010 that it had formed a partnership with FourSquare whereby: 'Metro will add their location-specific editorial content to the Foursquare service. People who choose to follow Metro on Foursquare will then receive alerts when they're close to one of those locations. For example, someone close to a restaurant that Metro has reviewed would receive a 'tip' about that restaurant and have the ability to link through to the full Metro review.'[56]

The E-Privacy Directive, Art 9 (implemented in the UK in almost identical terms by the *E-Privacy Regulations, reg 14*) regulates the use of location data. The key concern is where data indicates a specific location at a point in time (eg a Wi-Fi connection or a mobile phone with GPS) rather than a more general ongoing location (eg an IP address indicating a user based in the UK). The processing of such specific location data is permitted only if the user is anonymised, or has consented to such processing. Before consent is obtained, the user must be:

- told what location data is being used, why and for how long and whether it will be passed on to third parties; and
- given the opportunity, in a simple manner and free of charge, to withdraw consent at any time, both generally and for each individual communication. (Note that a service which asks a user once for their consent and never again might therefore not comply with this requirement. In any case, it is debatable whether a user would really be consenting to continued processing in such circumstances, as they may well forget that they had given consent at an earlier date.)

Processing of location data must also be restricted to what is necessary for the purposes of providing the 'value added service' (ie a service which requires the processing of traffic or location data beyond what is necessary for transmitting or billing a communication) for which the user has given their consent.

The ability of users to post location data on UGC sites is proving to be extremely popular – so much so, in fact, that there are concerns that users are compromising their own security by doing so. During early 2010, the website PleaseRobMe.com

[55] *DPA 1998, s 60(4)(c).*
[56] Metronews.ca, 25 January 2010.

extracted and republished location information posted onto Twitter by Foursquare users, explaining that 'the danger is publicly telling people where you are. This is because it leaves one place you're definitely not … home.' Nevertheless, the use of location data to provide relevant content is a quintessentially Web 2.0 idea which looks set only to increase in the coming years.

Privacy rights in the digital world

4.48 In view of the growing trend for interactivity and information sharing by users in the online world, it is ironic, but perhaps inevitable, that privacy issues are increasingly causing friction between data collectors and users. In recent years, perceived privacy violations have given rise to unwanted headlines for a number of high-profile businesses, including Facebook, Google and BT. But what does a right to privacy actually entail and how far does it extend?

Many data collectors direct users to their website privacy policies to demonstrate their commitment to privacy. Such documents generally set out what information will be collected about a user, how long it will be retained and the types of purpose for which it will be used. Despite the name 'privacy policy', such issues are actually more to do with compliance with data protection, a highly technical and well-defined area of law. Privacy is a more fundamental right, which comes down to the distinction between the public and private persona – in other words, the idea that some information is private to an individual by its very nature and should not be wrongfully used by anyone else. In fact, privacy is considered so basic a human right that it forms *Article 8* of the *European Convention on Human Rights* ('ECHR'): 'Everyone has the right to respect for his private and family life, his home and his correspondence'.

Is there a 'right to privacy' on the internet (or at all)?

4.49 A problem for the data-collector seeking to understand what the privacy laws prevent it from doing is that there is no clear definition of how far privacy rights extend. Although there is no standalone 'privacy law' on the English statute book and no separate tort of invasion of privacy under English law,[57] the *Human Rights Act 1998* ('HRA') requires courts, as far as possible, to construe English law in a way which is compatible with ECHR rights, including the *Art 8* right to privacy.

However very few privacy cases have been decided by the courts since the HRA came into force in 2000 (indeed, only two privacy cases were heard in the High Court in the two years since January 2008 and one of those settled five days into the trial[58]). Most privacy cases have concerned the publication of information about celebrities. The cause of action in such cases is breach of confidence, into which the courts have (reluctantly) 'shoe-horned' an assessment of how the celebrity's *Article 8* right to privacy weighs up against the publisher's *Art 10* right to freedom of expression.[59] The leading modern decision in the English courts was

[57] Confirmed in *Wainwright and another v Home Office* [2003] UKHL 53.

[58] *A and another v Priory Healthcare* (February 2008). The other case was Max Mosley's claim against the News of the World (*Mosley v News Group Newspapers* [2008] EWHC 1777 (QB)).

[59] *Douglas and others v Hello Limited and others* [2005] EWCA Civ 595, per Lord Phillips, MR at 53.

Naomi Campbell's claim against the Mirror newspaper for publication of photographs of her leaving Narcotics Anonymous meetings.[60] Lord Hope summed up the test that must be applied:[61]

> 'The underlying question in all cases where it is alleged that there has been a breach of the duty of confidence is whether the information that was disclosed was private and not public. There must be some interest of a private nature that the claimant wishes to protect … The broad test is whether disclosure of the information about the individual ('A') would give substantial offence to A, assuming that A was placed in similar circumstances and was a person of ordinary sensibilities … The law of privacy is not intended for the protection of the unduly sensitive.'

Reliance on case law to define the scope of privacy rights means that the concept of privacy remains something of a moveable feast. It should also be noted that privacy laws vary widely across Europe and other jurisdictions. For instance, in February 2010, an Italian court held three Google executives to be personally criminally liable for privacy breaches by the corporation, after a clip was posted by a user on Google's video service which featured the bullying of an autistic child – a decision described by the former UK Information Commissioner Richard Thomas as 'simply inconsistent with the way the internet works. There is no UK data law or European law that I know which could lead to this result'.[62] Considering the cross-border nature of many internet services, this inconsistency between national privacy laws is a cause for concern for e-commerce businesses.

In February 2010,[63] the UK Culture, Media and Sports Committee considered whether Parliament should introduce a law defining a right to privacy. It noted that there was no consensus as to whether privacy legislation was desirable or how it could be drafted, and it was concluded that a codified privacy law was not currently desirable:

> 'The Human Rights Act has only been in force for nine years and inevitably the number of judgments involving freedom of expression and privacy is limited … [but the] law relating to privacy will become clearer as more cases are decided by the courts … Given the infinitely different circumstances which can arise in different cases, and the obligations of the Human Rights Act, judges would inevitably still exercise wide discretion. We conclude, therefore, that for now matters relating to privacy should continue to be determined according to common law, and the flexibility that permits, rather than set down in statute.'

On this basis, and assuming that there were no issues of defamation, it is likely that any claim made by a 'normal' individual (ie a non-celebrity) that the use of information about them by a data collector infringed their privacy rights would have to follow the same cause of action as a privacy claim by a celebrity, namely by showing that:

60 *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22.
61 Ibid. at paras 92–94.
62 See www.independent.co.uk/news/world/europe/google-guilty-of-privacy-crime-in-web-test-case-1909915.html.
63 Culture, Media and Sport Committee – Second Report into Press standards, privacy and libel (9 February 2010)

- the information in question was genuinely private (which, if not obvious,[64] would require an assessment of whether the disclosure of the information would give substantial offence to the individual if they were a person of ordinary sensibilities);
- a duty of confidence existed between the individual and the data collector in relation to the information; and
- this duty was breached, causing the individual to suffer some loss or damage.

This is by no means an easy test to satisfy. For instance, what private information is misused and what loss does an individual actually suffer when a picture of the outside of their house is shown on Google Street View (especially as faces are automatically blurred and users can request the removal of inappropriate images)? Google has already won a case in the US against a Pennsylvanian couple who claimed that the inclusion of their house caused them 'mental suffering' and diluted the value of their home. The court concluded in that case that the claimants were 'unable to show that Google's conduct was highly offensive to a person of ordinary sensibilities'.[65] The view taken by many data collectors on the issue was summed up by Google's CEO, Eric Schmidt: 'If you have something you don't want anybody to know, maybe you shouldn't be doing it in the first place.' (It is, however, interesting to note Google's change of tone later in 2010 when it faced criticism and regulatory investigation for data which it had unintentionally collected from domestic wireless networks while mapping the Street View service. Google said in a statement that it was 'profoundly sorry' for collecting the data and promised to delete it as soon as possible.)

Privacy protests and the power of reputation

4.50 If ill-defined privacy rights hold little fear for data collectors in a strict legal sense, the power of reputation goes much further to shape privacy practices in e-commerce.

Given the amount of bad publicity that has surrounded privacy issues in recent years, data collectors are anxious to be seen to take privacy issues seriously. A sign of this is the somewhat cagey wording to be found in the privacy policies of many popular websites. (For example, Amazon's privacy policy opens with the words, 'Amazon.co.uk knows that you care how information about you is used and shared and we appreciate your trust in us to do that carefully and sensibly.') As a result, concerns about reputation can influence a data collector's whole approach to privacy issues.

Beacon – not a shining light

An example is the demise of Facebook's Beacon application. Beacon was launched in November 2007 and was heralded by Facebook as being 'a core element of the Facebook Ads system for connecting businesses with

[64] A blog is an example of a type of information which is obviously public and not private – *Author of a Blog v Times Newspapers Ltd* [2009] EWHC 1358 (QB) per Eady J at 11.

[65] *Boring v Google, Inc.*, 598 F. Supp. 2d 695, 699–700 (W.D. Pa. 2009). The privacy elements of the claimants' appeal against this decision were also later dismissed (*Boring v Google Inc.*, No. 09–2350 (3d Cir. Jan. 28, 2010)).

users and targeting advertising to the audiences they want.'[66] Beacon collected harvested data about the online activities of Facebook users on other participating websites, such as purchases made or products rated by those users, and sent that harvested data back to Facebook using third-party cookies. Originally, the system operated on an 'opt-out' basis so that unless the user actively opted out when asked whether they wished to share the information with Facebook, it was used for targeted advertising and was also transmitted to those other Facebook users listed as the user's 'friends'. There was no way to permanently opt out of the application.

Beacon was heavily criticised on privacy grounds by Facebook users, who launched a high-profile campaign through a Facebook group called 'Facebook, stop invading my privacy!' which gained 50,000 members within the first ten days.[67] Facebook responded by changing the application so that it operated on an 'opt-in' rather than 'opt-out' basis and introduced a permanent opt-out feature. However, despite these changes, Beacon continued to attract widespread adverse publicity. A class action lawsuit was filed against Facebook in the US,[68] which settled in September 2009 with Facebook agreeing to discontinue Beacon and pay $9.5 million to fund a non-profit foundation to promote online privacy, safety, and security.[69]

Several other examples of the bad publicity associated with perceived privacy breaches highlight the importance of the issue to data collectors:

- One of the most controversial aspects of BT's trial of Phorm's Webwise software in 2006–07 (see PARAGRAPH 4.8 above) was that the trials were carried out on BT customers without their knowledge (according to the European Commission, the company admitted as much in April 2008).[70] In view of the software's ability to track its users' web browsing habits, some users viewed this as a serious breach of their privacy. The European Commission has since stated that BT's trials had resulted in a number of complaints to both the ICO and the police.[71] On 6 July 2009, BT announced it had 'no immediate plans' to roll out the Webwise software to its broadband customers across the UK.

- Facebook faced another public outcry when it changed the terms of its privacy policy in February 2009, including the deletion of text which stated:

  'You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.'

  A blog called The Consumerist highlighted the potential significance of this change in a post entitled 'Facebook's New Terms Of Service: We Can Do

66 See www.facebook.com/press/releases.php?p=9166.
67 See www.facebook.com/group.php?gid=5930262681.
68 *Lane et al v facebook, inc et al*, case no 5:08-CV-03845-RS.
69 See www.beaconclasssettlement.com/FAQs.htm.
70 Commission Press Release IP/09/570 (14 April 2009).
71 Ibid.

Anything We Want With Your Content. Forever.'[72] which received substantial media coverage across the world. Within three days, Facebook had reverted to the previous version of its privacy policy and reinstated the deleted wording.

- Yet another privacy furore emerged with the launch of Google Buzz in February 2010. When users logged into Buzz, a social networking application, the application was set up so that they would automatically be 'following' (ie linked to) their most frequent contacts from Google's email and instant messaging services. Concerns were raised that Buzz's default settings meant that a user's list of contacts was made public (meaning that third parties could discover who the user had sent emails to in the past) and that in certain circumstances this list might even reveal a contact's email address. Google was forced into a public apology four days after the launch of Buzz, and made changes to the application to address the issues raised.[73]

Privacy in the online world is a fast-developing area, and one where the law has often been slow to keep up with the twin tides of technological development and public opinion. As the above examples show, public opinion and the threat of litigation or regulatory investigation (together with the associated threats to the reputation of data collectors) are more commonly the determining factors for digital privacy practices. Ultimately, on 'the notoriously fickle internet, where today's cultural icon is tomorrow's passing fad',[74] maintaining goodwill and popularity is essential for an online business's survival. Peter Fleischer, Google's Global Privacy Counsel, summed this up in 2008:

'At Google, our success depends on trust. If our users don't trust us, they won't use our services. And they won't trust us if we don't protect their privacy … our users are just one click away from switching to a competitor's services.'[75]

Data retention

4.51 Data retention is an issue with privacy implications for certain types of data collector. As part of the EU's counter-terrorism measures, the *Data Retention Directive* (2006/24/EC) imposed obligations on 'public communications providers' (principally ISPs, notified of their obligation by the Secretary of State) to retain records of certain types of communication information. The UK implemented the retention rules relating to internet access, internet telephony and email in the *Data Retention* (*EC Directive*) *Regulations 2009*. The measures are intended to assist criminal investigations and an investigating authority can issue a notice under the *Regulation of Investigatory Powers Act 2000, s 22* for disclosure of the records, subject to satisfying the requirements of that section.

The Regulations require affected data collectors to retain information such as user identification numbers, IP addresses, names and postal addresses of users, dates

[72] See http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html.

[73] See http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html.

[74] Many online businesses have a limited shelf life at the best of times (eg consider the rapid rise and fall of other social networking sites: www.guardian.co.uk/technology/2009/mar/29/myspace-facebook-bebo-twitter.

[75] Speech to European Parliament Committee on Civil Liberties, Justice and Home Affairs Public seminar: Data Protection on the Internet (21 January 2008) online at www.google.com/events/docs/policyblog_peter_fleischer_statement.pdf.

and times of login and log-off, and email addresses of the recipients of emails, are retained for a period of 12 months from the date of the communication in question. There is no requirement to retain the content of emails or calls.

Conversely, privacy campaigners often complain that data collectors retain users' data for too long. Search providers such as Google, Yahoo! and Microsoft have all introduced data retention policies whereby IP address and cookie data stored alongside search results is deleted after a certain period of time. For example, Google currently anonymises ad-serving and other log data after nine months and its ad-serving cookies expire after 18 months, while Microsoft announced in January 2010 that it would reduce the retention period for IP addresses associated with Bing search queries to six months.[76] However, in May 2010, the Article 29 Working Party wrote to Google, Microsoft and Yahoo! expressing concerns that the companies' data retention policies still did not go far enough to comply with European Law. Reuters also reported that the Article 29 Working Party wrote to Google in February 2010 asking it to halve its retention period for unblurred Street View images to six months.[77]

For data collectors who are not subject to the legal data retention requirements described above, and in relation to types of data which fall outside the scope of those regulations, the issue comes down once again to a balancing act between a data collector's commercial and technical interests in retaining data and its desire to keep a good reputation for privacy.

Key Messages

- While data protection has traditionally been seen as a 'compliance-only' issue, the reputational effects of not addressing privacy matters properly can be severe and dramatic. This is exemplified by the demise of Facebook's Beacon application and BT's trial of Phorm's Webwise software.
- Any business operating internationally needs to consider that data protection laws are not interpreted or enforced equally across the EU. In particular, in France and Germany, local regulators will seek to enforce more stringently the terms of the Data Directive and advice should be sought in these jurisdictions.
- All businesses should be aware of the change to the law regarding cookies to take effect by 25 May 2011 as a result of an amendment to the *E-Privacy Directive, Art 5(3)*. This (at least in theory) will require users to consent to the use of cookies when used for non-administrative tasks on websites and in particular will affect the use of targeted advertising. Organisations using behavioural advertising or offering ad serving will need to watch closely the guidance published by regulators relating to this issue.
- There is a higher standard required for electronic direct marketing (as opposed to non-electronic direct marketing) as a consequence of the *E-Privacy Regulations*. Organisations should familiarise themselves with the 'soft opt-in' exemption which enables direct marketing to users without needing consent.

[76] See http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx.

[77] See www.reuters.com/article/idUSLDE61O2QH20100225.