At the time of writing, the Advocate General and Court of Justice in the *Schrems v Commissioner* case, has put the nail in the EU–US Safe Harbour personal data transfer agreement. Lawyers, policymakers as well as an international technology sector are keenly considering what happens now after the Court of Justice decision.[1] The agreement is invalid. This invalidates the transfer of personal data from the EU to the US. This has major implications.

1 *Schrems v Commissoner*, Case C-362/14, AG Bot, 23 September 2015, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1395932669976&uri=CELEX:62014CC0362.

CHAPTER TWO

Contract

> 'The customer pays his money and gets a ticket. He cannot refuse it. He cannot get his money back. He may protest to the machine, even swear at it. But it will remain unmoved. He is committed beyond recall. He was committed at the very moment when he put his money into the machine.'
>
> Lord Denning, *Thornton v Shoe Lane Parking*[1]

2.1 That Lord Denning's comment should have perhaps more resonance to the average person today than it did in 1970 is largely attributable to electronic commerce – or 'e-commerce'. In 2014 British consumers spent £104 billion buying goods and services online. Disregarding business-to-business e-commerce dealings, proof, if it were needed, that in comfortably under two decades, through rapid development and refinement, e-commerce is now a fact of our everyday lives and still ignoring the vast sums spent online in business to business dealings.

Whatever financial or societal reasons are given for this, whatever 'paradigm shifts' are held responsible, one fact is certain: if consumers and businesses did not believe that the transactions into which they entered were legally enforceable, they would simply eschew the vast marketplace provided by the internet. This chapter will consider how English contract law applies to consumer and business contracts entered into using the internet.

The internet gives businesses access to a vast number of consumers, gives businesses access to each other and, increasingly, opportunities for individuals to meet each other and even to create, publicise and share their own content. The first large-scale consumer and business use that was made of the web was the erection of websites for marketing and advertising purposes. These sites acted primarily as a shop window, informing potential customers of the *existence* of companies and their products or services but not offering the possibility of selling them. Sales were concluded in parallel through more traditional means of communication. As websites have become more sophisticated and high-quality graphical and interactive content has become the norm, commercial websites have morphed into particular online environments providing not only space for near limitless 'window' shopping but also crucially, embedding the means

1 [1971] 2 QB 163 at 169.

to select products, conclude contracts for them and securely make payment. Websites not only offer convenience and immediacy for consumers (and in the case of software, for example, immediacy of delivery) and a wider audience for sellers, they have also transformed the way that businesses transact with each other, providing specialised platforms for procurement and payment and the management of purchasing.

These commercial benefits create novel issues for contract law.

FORMATION OF CONTRACT

2.2 In the main this chapter does not consider the terms of a contract made over the internet; the main concern is to analyse the validity of contracts made over the internet. This is an important distinction. Under English common law, an agreement becomes legally binding when four elements of formation are in place: offer, acceptance, consideration and an intention to create legal relations. In some circumstance these can be clearly identified, discrete elements that fall into a broadly chronological and linear sequence, which may be preceded by an invitation to treat, although the four elements may be found without necessarily going through each of these.

For contracts entered into over the internet (or other 'information society service', therefore including mobile services as well as interactive television offerings), the UK's Electronic Commerce (EC Directive) Regulations 2002 ('Electronic Commerce Regulations')[2] and Consumer Protection (Distance Selling) Regulations 2000 ('Distance Selling Regulations'),[3] together with certain other content-specific regulations, introduce new pre-contract formalities, in particular for consumers and, in the case of the Electronic Commerce Regulations, businesses which do not agree otherwise. Along with these formal requirements, law, statute and a body of regulatory and self-regulatory codes and guidance prescribe the content of a contract. For example, an e-commerce contract may be validly formed, but one of its terms may be ineffective under other rules. This section focuses on the formation of a contract, examining each of the four elements and key stages in turn, and highlights those additional features specific to the internet of which businesses and their advisers should be aware.

Contracting via the internet

2.3 There will usually be no reason why a contract may not be formed over the internet, whether via a website, email or other form or electronic communication, such as a live online 'chat', provided that each of the four elements required to

2 These Regulations implement Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the Internal Market, OJ L179/1 ('Electronic Commerce Directive').

3 This Regulation implements Directive 97/7/EC on the protection of consumers in respect of distance contracts. See Chapter 9 for analysis.

form a valid contract is satisfied. Indeed, the Electronic Commerce Directive requires all member states to ensure that their legal systems allow contracts to be concluded by electronic means and that any legal obstacles to the process are removed.[4] Steps have been taken by the UK government to provide for this, as considered below.

There are, however, exceptions to this principle that contracts may equally be made using digital means as with more traditional (tangible) mediums. These exceptions are: (i) where the parties have agreed that a contract (or amendments to it) must be formed otherwise (in which case there will not be requisite intention to be bound if this is not followed); and (ii) where there is a statutory requirement that a document or agreement must be in a specific format. Each is considered below.

Stipulation by the parties

2.4 There may be various reasons, public policy or otherwise, why parties may choose to contract or amend contracts in a format other than via the internet. In most situations this will be because parties desire evidence and a physical record of the contract. In others, it will simply be because this is the way they 'have always done things'. Although the use of technical means (such as a pdf to seek to prevent a document from being amended, and digital signatures – see **2.52**)), and the fact that email communications are now commonplace in disclosure, have gone a long way towards assuring parties that they will have robust evidence in the event of a dispute, some still prefer to seek reliance on paper contracts and records.[5]

Whatever the parties' choice, it is essential that this be made clear. Those who draft and review contracts are urged to consider references to 'writing' carefully, to ensure that email correspondence is included or removed as required, and clearly exclude electronic contracting or amendments if this is intended. The decision in *Hall v Cognos*[6] provides a useful warning on this point. In this case, Mr Hall failed to submit an expenses claim within the stipulated time limit. In response to an email requesting an extension, Mr Hall was told 'okay' by his manager. The company subsequently refused to grant the extension and Mr Hall brought a claim against them. The court held that the claims policy, which formed a part of Mr Hall's contract of employment, (which stated that any variations had to be 'in writing and signed by the parties') had been varied by the email. The email constituted writing and the printed name of the sender at the top of the email was judged a signature. This case sends out a further warning to parties on the use of email for making binding contractual statements since, in this case, the manager who emailed back the confirmation did not even have authority to agree the variation. However, he was held to have ostensible authority sufficient to bind the company.

4 Recitals 34 to 38 and art 9.

5 Indeed this may be a stipulation of some companies' insurance policies.

6 *Hall v Cognos Ltd* (unreported, 1997).

In *Pretty Pictures v Quixote Films*,[7] email communications were held not to bind the parties to a contract, since the emailed statement said that 'I hope we now have a deal. I look forward to your confirmation and receiving a deal memo by fax.' Although the other party said that the 'deal is now approved' and that he would send the contract by email, the judge held that there was no binding contract. This was because the common intention of the parties was that the contract would only become binding when each signed some form of memorandum or other paper copies to be given or exchanged, or if the contract were amended to provide for electronic signing, communication or delivery (see **2.52** below for further details in relation to digital signatures).

By contrast, in *Immingham Storage Co Ltd v Clear plc*[8] the Court of Appeal held that a contract was formed by an exchange of emails notwithstanding that the signed quotation returned by email to the offeror, which was held to have been accepted and formed a binding agreement with the offeree stated that a 'formal contract will follow in due course'.

The problem illustrated in these cases is a failure to clearly identify not just the means by which a contract is made but the documents that will form that contract, a problem illustrated in *Von Hatzfeldt Windenburg v Alexander*[9] and implicitly noted by Lord Wright in *Hillas v Arcos*.[10] It is not therefore a novel one, or one directly related to the use of electronic communications. Notwithstanding the differing outcomes in these cases, they are all evidence of the need for parties to be clear in identifying the 'medium' by which their contract is to be made to avoid both uncertainty and potentially costly litigation.

Statutory requirement

2.5 The Electronic Communications Act 2000 gives Parliament the right to amend old statutes which specifically require the use of ink and paper, in order to facilitate electronic commerce. Some statutes have already been changed through regulation in this way. An example is the Consumer Credit Act 1994 (Electronic Communications) Order 2004, amending the Consumer Credit Act 1974, to enable consumer credit agreements to be concluded and most notices and documents[11] to be provided by electronic means. This removes the prior requirement that they must be in paper form.

However, the Electronic Communications Act still requires that each statute be amended in turn. With this piecemeal approach, some statutes still remain unamended. It remains important that parties consider whether there may be

7 *Pretty Pictures v Quixote Films Ltd* [2003] EWHC 311 (QB).
8 *Immingham Storage Co Ltd v Clear plc* [2011] EWCA Civ 89.
9 *Von Halzfeldt Wildenburg v Alexander* [1912] 1 Ch 284.
10 *W N Hillas & Co Ltd v Arcos Ltd* [1932] UKHL 2 at [10] per Lord Wright.
11 Note that default, enforcement and termination notices have been singled out (by way of the Consumer Credit (Enforcement, Default and Termination notices) (Amendment) Regulations 2004) as a special case and still retain a requirement that they be provided in paper format since such notices are deemed to have significant impact on the rights of debtor and hired. The assumption is that default is likely to be due to financial hardship which in turn means that the individual may no longer have access to electronic communications.

any statutes that apply to the subject matter of such contract and its form which would require that specific requirements be followed.

It should be noted that, where legislation simply refers to a requirement that something be 'in writing', without any other requirement (ie the statutory context is neutral as to the medium and does not, for example, refer to the need for paper copies), the Interpretation Act 1978 states that:

> 'Writing includes typing, printing, lithography, photography and other modes of representing or reproducing works in a visible form, and expressions referring to writing are construed accordingly.'[12]

The Law Commission's interpretation of this is that:

> 'Writing includes its natural meaning as well as the specific forms referred to. The natural meaning will include any updating of its construction; for example, to reflect technological developments.'[13]

With this in mind and considering the extent to which electronic 'writing' is now pervasive, it is difficult to foresee that electronic communications such as emails or website order processes could fail to constitute 'writing'.

Of course, in the majority of contracts, particularly in the electronic commerce arena, there will be no statutory requirement providing for specific forms, whether in writing or otherwise. To this extent, general common law principles will apply and it is clear from a number of cases, that there is no reason why a contract may not be concluded via electronic means, provided that the requisite elements are met.[14]

Pre-contract information

2.6 The Electronic Commerce Directive and its implementing legislation oblige almost every owner of a website established in the European Economic Area (EEA) to provide certain information to its visitors, whether the website permits transactions or not, and regardless of whether users of the website are acting in a consumer or business capacity. These requirements fall outside the established elements of contract formation in requiring an additional layer of information to be provided for internet services.

In the UK, further information requirements apply pursuant to the Companies Act 1985 (as amended pursuant to the Companies Act 2006[15]), and the Business Names Act 1985. These require that a company (and in respect of the Business Names Act 1985, also a partnership or other trading entity) registered in England

12 Interpretation Act 1978, Sch 1.
13 Para 3.7, 'Electronic Commerce: Formal Requirements in Commercial Transactions, advice from the Law Commission, December 2001'.
14 See, for example, *Hall v Cognos Ltd* (unreported, 1997) and *NBTY Europe Ltd (Formerly Holland & Barrett Europe Ltd) v Nutricia International BV* [2005] All ER (D) 415 (Apr).
15 Amendments were made to ss 349 and 351 of the Companies Act 1985 pursuant to the Companies Act 2006 and the Companies (Registrar, Languages and Trading Disclosures) Regulations 2006.

and Wales place certain key contact and other particulars regarding the company on all of its websites and in official business correspondence. Companies are generally advised to include it in all email correspondence by default to avoid the need to determine whether it is actually a business email or not.

We examine the Electronic Commerce Directive requirements in this chapter by first assessing where a website owner is 'established'. We then consider the manner of provision and nature of the information which EEA-established entities must make available to all visitors to a website. Finally we analyse the nature of the additional 'transactional' information that may need to be provided prior to orders being taken.

Establishment of providers

2.7 The Electronic Commerce Directive does not have extraterritorial reach; it binds only member states, meaning here, those established within the EEA (EU Member States with Iceland, Liechtenstein and Norway). The concept of establishment, however, in relation to websites, is problematic. Large websites are often hosted simultaneously on multiple servers which may be situated anywhere on the planet and may be used interchangeably. Consequently, they may be many thousands of miles from where those who control them are physically established.

Location of servers not conclusive

2.8 The Electronic Commerce Regulations, which implement the Directive, however, take a pragmatic view of establishment:

> '"established service provider" means a service provider who is a national of a Member State or a company or firm as mentioned in Article 48 of the Treaty and who effectively pursues an economic activity using a fixed establishment for an indefinite period, but the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider …'[16]

In effect, therefore, the location of one's servers does not change where one is established. The question of establishment is first one of from where the economy activity of a fixed establishment is being pursued. Having determined this, one must then determine whether or not the use of the fixed establishment is for an indefinite period or not. Employees working in a leased building are the sort of situation envisaged here. One cannot conclude anything from the mere fact that servers are, or are not, inside the building.

Multiple establishments

2.9 Complications arise where more sophisticated companies have multiple locations providing support to a particular website. For example, a company with a website could be headquartered in Japan but technical control and maintenance

16 Reg 2(1), part definition.

of the site is undertaken by a team based in California, while, all the content on the website is created by a group of freelance Irish web designers which posts finished articles to an editor in an office in Dublin, and customer support is handled from the UK. The site's credit card processing is conducted in Germany and all goods are shipped from local distribution centres around the world. In this scenario, determining where the company is established is not straightforward.

The Electronic Commerce Regulations and Electronic Commerce Directive clearly envisage such a scenario. We are told, 'in cases where it cannot be determined from which of a number of places of establishment a given service is provided, that service is to be regarded as provided from the place of establishment where the provider has the centre of his activities relating to that service'.[17]

In the scenario above, therefore, the place of establishment on this basis may well be considered to be Japan because this is where the main base is. However, there is a concern associated with this definition being used to interpret where a multiple-state-located service provider is established for the purposes of the Electronic Commerce Directive and Electronic Commerce Regulations. The recital and definition would seem to suggest that different services may have different centres of activities relating to them. What follows from this is the possibility that the service of, say, ordering a product from a website is centred within the UK but the service of delivering it is centred in the US. In other words, one service is EU-centred; the other, from the same website, may not be. In such circumstances, the service provider may be unsure whether the legislation applies. In the first scenario, therefore, the management services undertaken in Japan may be viewed as separate to the Irish editorial service and UK customer support. As will be explained, the contractual sanctions for not complying with the Electronic Commerce Regulations are potentially severe enough that any UK service provider is advised to assume that they are established in the EEA, for the purposes of the Electronic Commerce Regulations.

General information to all

2.10 If a service provider is established in the EEA, they must make available certain general information about themselves. This information must be made available to the recipients of their service (ie a website) 'in a form and manner which is easily, directly and permanently accessible'. If a service provider fails to do this, they may be liable in damages by their visitors for breach of statutory duty.[18]

Alongside this, the information requirements contained in the Companies Act 1985 (as amended) and the Business Names Act 1985 in relation to websites and emails duplicate the requirements previously required in respect of business stationery and other documents. Such information must be legible. Failure to comply with these non-Electronic Commerce Regulations requirements is a criminal offence carrying a fine of up to £1,000.

17 Reg 2(1). Recital 19 is similar.
18 The Electronic Commerce (EC Directive) Regulations 2002, reg 13.

Information to be made available

2.11 The scope of the information to be made available pursuant to the Companies Act 1985 consists of the company name, place of registration (ie England and Wales), registered number and registered address. The Business Names Act 1985 requires that, in the case of a partnership, the name of each partner, in the case of an individual, his name and, in the case of a company, the corporate name, is given clearly and legibly.

The information required under the Electronic Commerce Regulations (discussed below) is as follows:[19]

1. the name of the service provider;
2. the geographic address at which the service provider is established;
3. the details of the service provider, including his electronic mail address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner;
4. where the service provider is registered in a trade or similar register available to the public, the register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
5. where the provision of the service is subject to an authorisation scheme, the particulars of the relevant supervisory authority;
6. where the service provider exercises a regulated profession:
   (i) the details of any professional body or similar institution with which the service provider is registered;
   (ii) his professional title and the member state where that title has been granted;
   (iii) a reference to the professional rules applicable to the service provider in the member state of establishment and the means to access them;
7. where the service provider undertakes an activity that is subject to value added tax, the VAT number; and
8. where prices are referred to, these shall be indicated clearly and unambiguously and, in particular, shall indicate whether they are inclusive of tax and delivery costs.

Again it should be stressed that this information must be provided regardless of whether the website in question is transactional or not.

Form and manner of information

2.12 The above information must be 'made available to the recipient of the service … in a form and manner which is easily, directly and permanently

19 The Electronic Commerce (EC Directive) Regulations 2002, regs 6(1)(a)–(g) and 6(2).

accessible'.[20] Unlike specific transactional information mentioned below, the above information may be made available at any time during the encounter with the website visitor. This said, one should note that this information must be 'easily' accessible. Burying the information after numerous other pages on a website is unlikely to satisfy this requirement. A link from the homepage to a list of this information is probably the most obvious way to make the information available. Some website operators may choose to include this information within their standard 'Terms and Conditions'. This too is likely to be acceptable but with one caveat. This information must be made available 'permanently'. Consequently, websites must not be designed so that the information is, say, only available while one is conducting a particular activity or about to finish placing an order. The information must be able to be accessed even after a visitor has enjoyed the site. Another common place to position this information on non-transactional sites is in an 'About Us' or 'Contact and Legal Details' section.

> *Example 2.1*
>
> An online news service has a subscription service: individuals pay £15 each month to access the service's database of past news articles. The Electronic Commerce Regulations' 'General Information' is made available through a link to the right of the search area on the site. The link is called 'About Us', but the page on which it is housed is only accessible during the course of a paid month and not afterwards. It is therefore arguable that the information is not 'permanently' accessible and so is non-compliant.

Transactional information prior to order

2.13 If a service provider is established in the EEA and is soliciting orders from visitors to its website, it must provide specific information about its transactions to potential consumers and businesses (additional requirements specific to consumer-only transactions are considered separately in this chapter) who do not agree otherwise. This information must be provided to the recipients of their service 'in a clear, comprehensible and unambiguous manner'.

If a service provider fails to do this, they may be held liable by their visitors for damages in breach of statutory duty.[21] In addition, they must allow a consumer to identify and correct input errors prior to placing their order. If the service provider does not make this facility available, the consumer may rescind the contract.[22] Should the customer so cancel, the service provider may apply to the court to order that the consumer may not rescind the contract.'[23]

Website owners and their advisors are therefore strongly advised to pay particular attention to the following section. An owner of a website may well choose to ignore the requirement to make available the general information. If they do so, they are taking the low-cost risk of an action for damages for breach

20 Reg 6(1).
21 Reg 13.
22 Reg 15.
23 Reg 15.

of statutory duty. Few website owners, in contrast, can afford to run the risk that any of their contracts could simply be rescinded by the customer at any time.

Provision of information in clear, comprehensible and unambiguous manner

2.14 The scope of the information to be provided in a 'clear, comprehensive and unambiguous manner' prior to the order being placed is simple to understand.[24] It nevertheless may be complex to implement and include on certain websites. The six headings below detail the information required and special concerns of each requirement.

Technical steps to conclude contract

2.15 Regulation 9(1)(a) provides that a website must provide for the user of the website the steps which will result in the conclusion of a contract. The most clear and comprehensive way for this to be achieved is by the use of a 'crumb trail' at the top of the ordering section of the site. A 'crumb trail' is a line of text showing all the steps needed to enter the contract with the current step highlighted. Having, say, 'Choose – Provide Credit Card – Confirm' at the top of the screen certainly does go some way to be clear and comprehensive. What is needed in addition, however, is some explanation of the meaning of each of these steps. A link from each with a short description would ensure that the 'crumb trail' is not ambiguous as to, for example, when the order is complete.

Filing of concluded contract

2.16 Website owners are obliged by reg 9(1)(b) to provide information before the order is placed as to whether or not the concluded contract will be filed and, if so, whether it will be accessible. Although it is obviously trivial to state this in such a way as to comply with the Electronic Commerce Regulations, it may be more difficult to comply with the actual statement itself.

Many websites allow a user to access their previous orders. This, however, is only one aspect of the concluded contract. The other aspect is the text of the contract itself incorporating the prevailing Terms and Conditions from the website. The difficulty here is that these terms and conditions are subject to frequent changes and the current terms to which a user may now have access may not be the same terms on which they contracted. To comply with the filing requirement, therefore, customers must be able to continue access the historical Terms and Conditions used to conclude each order. This may be onerous and as such, most websites will generally elect to state that the contract will not be filed.

How to identify and correct input errors

2.17 Regulation 9(1)(c) obliges websites to provide in a clear, comprehensible and unambiguous manner information about how customers may identify and correct input errors before they place an order. In addition, the website is obliged

24 Reg 11.

to make available 'appropriate, effective and accessible' technical means to identify and correct input errors.

The easiest way to comply with this is to require a user either to confirm an order and ideally to allow them adjust it. There is unlikely to be a problem so long as the customer is left in no doubt that the order details on the confirmation page of the ordering procedure may be rejected, and then altered, or accepted. Many websites go further to allow confirmed orders to be modified before goods are dispatched.

> *Example 2.2*
>
> CD410.co.uk is a website which sells music CDs for no more than £10 each. Its designers omit to alter their ordering pages to allow individuals to correct input errors. Instead, by the 'Confirm' button, they state: 'Don't worry if you've made a mistake and have ordered the wrong thing, simply pop it back unsealed in the post to us with 30 days and we'll credit the money back to you!' In this scenario, CD410.co.uk will not have complied with the requirement to allow individuals to correct errors before they place their order; each customer will be able to rescind the contract at any time not only within their stipulated 30 days.

Languages offered for contract

2.18 Finally, reg 9(1)(d) requires that websites must provide details of the languages that are offered for conclusion of the contract. There is no stipulation that a website must contract in a range of languages merely that where alternatives are available this is drawn to the attention of users.

Relevant codes of conduct

2.19 Many website operators are members of voluntary or mandatory codes of conduct. Where this is the case, a list of these must be provided prior to the order being placed, together with information about how to consult the codes electronically.[25]

Terms and conditions for storage and reproduction

2.20 It is sensible for most websites to allow each customer to see the site's terms and conditions before they can place an order. If they cannot see the terms and conditions, there is a risk that a court will deem that the terms and conditions (or at least some of them) have not been 'incorporated' into the contract with the customer. This is discussed below.

Where terms and conditions are provided, the Directive and Regulations impose a further obligation that the website operator must make the contract available to the recipient in such a way that allows him to 'store and reproduce' it.[26] Historically, simply allowing the user to print the terms would suffice but as desktop printing becomes less common and crucially as websites are accessed

25 Reg 9(2).
26 Reg 9(3).

CHAPTER FOUR

Intellectual property

'[T]he internet is the world's biggest copying machine.'

Marybeth Peters, Register of Copyrights, 1995[1]

4.1 The material stored and transmitted through the internet is intangible and much of it will be protected by intellectual property rights. These rights can protect the intangible but substantial assets of companies and creative products of the mind from damage and unauthorised use. This chapter focuses on two of these rights: trade marks and copyright.

A trade mark or a brand name is forever important to businesses and consumers. For businesses the goodwill built up through sales under a brand can be extremely valuable. For consumers, a trade mark indicates the source of a product and so indicates its quality. It is therefore crucial that where e-commerce takes to the internet, where it is easy to fake an identity, the law protects trade mark owners and consumers from imposters. This is crucial in the area of domain names.

Copyright protects almost all the material used and transferred over the internet and the World Wide Web. This right can protect emails, websites and the programs and content shipped across the internet. It is therefore relevant for users and internet service providers to understand the ambit of these rights and what activities will lead to their infringement.

TRADE MARKS, DOMAIN NAMES AND PASSING OFF

4.2 A webpage provides a business with both a method of advertising and a method of selling to customers. The difference between any other advert and one on a website is that the nature of the internet means that the advertisement can be viewed anywhere by anyone.[2] This provides incredible commercial benefits

1 US News and World Report, 23 January 1995, at p 59.

2 Geo-blocking technologies are becoming increasingly effective, and courts are starting to require website providers to institute location-sensitive access. However, the European Commission appears to be against using such technical measures: See Press Release: *Digital Single Market,* 25 March 2015 (IP/15/4653).

to a business, as it no longer has to have any local physical presence to sell to customers. But in both the real world and the virtual world, trade marks and branding are essential. The potentially global reach of the internet, however, makes issues about trade marks far more complicated than was ever previously the case. This first part of the chapter will look at trade marks, in particular how domain names can be used as trade marks. It then moves on to consider passing off and its application to domain names through the instrument of fraud doctrine. It then considers the special arbitration rules which apply to domain names.

Technical rights v legal rights

4.3 As early as 1994, domain name disputes were starting to appear in courtrooms. In *MTV Networks v Adam Curry*,[3] Adam Curry had beaten the famous Music Television Network to a domain name. Before August 1993 he had registered and operated a website with the domain name 'www.mtv.com'. This site provided information about the music business, and dovetailed with the television business of MTV. On 19 January 1994 MTV sought to acquire the domain name. By spring 1994 millions of internet users had accessed the 'www.mtv.com' site. This is a common scenario in domain name clashes. The only right which Adam Curry had over the site was a technical one: he was the owner of the domain name alias: he was not the owner of any legal rights to use the name (or trade mark) MTV.

This problem is also affected by the fact that although there can be only one '.com', there has always been the risk that there may be many variations of the domain name with different suffixes (TLD). For example, in November 1993 Merritt Technologies Inc was granted the domain name 'mit.com'. From 30 December 1993 Merritt used the domain to provide free internet access to the handicapped, disabled and elderly. On 6 May 1996, Merritt received a letter from the Massachusetts Institute of Technology asking Merritt to select an alternative domain name. Their rights to insist upon this were based on their use of the MIT trade mark since 1861, having a worldwide reputation and five registered trade marks in classes unrelated to Merritt's use of the mark. The Institute already owned the domain names 'mit.org' and 'mit.edu'. There was no crossover in fields of activity: the Institute was simply worried that its trade mark was being used at all. This is now a routine occurrence. This is because the naming committees both here and elsewhere are expanding, and will continue to expand, the numbers of suffixes (TLDs) available; but as the late Jon Postel of the Internet Assigned Name Authority (IANA) wrote:[4]

> '[T]he trade mark issue is just a mess. McDonalds is going to want to have mcdonalds.com, mcdonalds.biz, and other domain names involving McDonalds.'

3 867 F. Supp 202 (SDNY 1994).

4 Information Law Alert, 02/09/96, 'Antidilution trade mark law gets first court case'.

This chapter looks at the conflict between legal rights in cyberspace, where in most cases little has really changed, and the conflict between technical rights (in domain names) and legal rights (in trade marks).

The nature of trade mark protection

4.4 Trade marks are, like all intellectual property rights, territorial by nature. This means that a person who registers a trade mark at the Intellectual Property Office is entitled to protection for that trade mark only within the United Kingdom and the Isle of Man. Such a person is only entitled to protection in other countries where separate applications are made in those countries. This means that a trade mark can be owned by two entirely separate and unrelated entities in two different countries; for example, one business could own the mark 'DOG' for clothing in the US, and another could own and use 'DOG' on clothing in the UK. The territorial nature of trade marks means that, in the real world at least, there is no overlap of rights as each trade mark owner can operate only within the geographic territory where they have rights.

In addition, a trade mark only grants protection in relation to the goods and services in respect of which it is registered. This means that two traders can use the same mark for different goods in the same marketplace (eg 'Green' used in respect of musical instruments by one trader and in respect of footwear by another) without infringing each other's rights. In such cases, therefore, there is no conflict of rights. It is also possible for two traders to agree between themselves that they can both use the same mark in respect of the same goods in the same (or part of the same) marketplace (co-existence agreements).

Trade marks are not unique. It is possible, therefore, to have conflicts between trade mark rights where two trade mark owners (one from the US, one from the UK) both use the mark on the internet at the same time. The nature of the internet also means that problems may arise in relation to genuine goods which are sold under the trade mark, but which have yet to be put on the market inside the EU (ie parallel imports). This can cause problems when consumers see products (eg jeans) are on sale on a US website for less than they are sold in the UK, and then seek to buy from abroad. The basic questions of trade mark law which these businesses face, however, is little different from real world activities. The nature of the internet raises different matters only in some areas. It is these areas which this chapter concentrates on, but a general introduction to trade mark law is included although those wanting answers to more technical questions should consult a specialist text.

Domain names

4.5 Every computer on the internet has an IP (Internet Protocol) address. These addresses are made up of a series of numbers, which have the form 123.45.678.910.[5] The numbers can be assigned permanently or temporarily

5 This is an IP version 4 address of the type used by virtually all networks.

(floating), for example most home users of the internet have a new IP address allocated by their internet service provider every time they log onto the internet. In contrast, businesses often have a permanent IP address for the server; although users of the business's network might have a temporary address.

The problem with IP addresses is that they are not very easy to remember.[6] To remedy this problem a sort of phone directory was set up which assigned a name to every IP address. This meant that instead of typing up to a 12-digit number, users could type a domain name ending with one of the so-called generic top level domains (.com, .org, .net, .biz, .tv) (gTLD) or one of the country code top-level domains (.uk, .fr) (ccTLD). Where a domain name has a ccTLD[7] (eg lawyer.co.uk) it does not necessarily mean that the user of that domain name is in the UK or that the server where the material is stored is in the UK. A postal address necessarily changes whenever one moves from one town to another, but a domain name may remain the same wherever one moves. The only way to locate the owner of a domain name is to geographically locate the internet protocol address.[8]

Domain names, like company names, are not simply taken; they are registered. They are also unique (so www.flower.com is different from www.flowers.com) and so no two people can separately own the same domain name. Most registration companies do not check that an applicant has the right to use a particular name as a domain name and so the registrars allocate them on a first-come, first-served basis. In the UK, this approach was been approved of (or at least accepted) by the court in relation to the domain name 'pitman.co.uk'.[9] It was concluded that because the claimant, Pitman Training Ltd had no rights to proceed for passing off or any other tort, Nominet (responsible for 'co.uk' domain names) was entitled to register domain names as and when they are requested by an applicant and did not have to investigate entitlement in advance.

Trade marks v domain names

4.6 The unique nature of each domain name means that unlike trade marks there is no way to exercise rights independently of each other. There can only be one apple.com despite both Apple and Apple Records both wanting to use the name and, until the launch of iTunes, there being only limited overlap between

6 Because the domain name which humans remember and type merely 'refers' to a unique number, it is possible to expand the quantity of IP addresses without having to alert consumers to the change. This is clearly different from telephone numbers where, if extra numbers are required to allow for growth, every existing number must change. At present most IP addresses still use version 4 (which uses 32-bit binary numbers). It is possible for a network to change to using IP addresses using version 6, which is a 128-bit hexadecimal number. Although this format is not widely used, when it is adopted it will not change domain names and most users will be totally unaware of the change.

7 There are also a number of quasi-ccTLDs, such as '.uk.com'. These are not actually ccTLD, but are privately owned sub-domains in the gTLD '.com'. Accordingly, 'uk.com' is registered as a domain name and if there were 'IPlawyer.uk.com' then if the 'uk.com' domain name is not renewed all those relying on sub-domains would lapse at the same time.

8 There are a number of geo-locating websites, which can provide details of where a particular site was accessed from.

9 *Pitman Training Ltd v Nominet UK* [1997] FSR 797.

the businesses. In contrast, Apple can own the trade mark in relation to some goods and services whereas Apple Records can own in relation to others without there necessarily being any conflict of the rights.[10] John Gilmore of the Electronic Frontier Foundation sums up the issue well:[11]

> 'Trade marks are registered in a system that permits many companies to share a name legitimately without interfering with each other, such as Sun Photo, Sun Oil and Sun Microsystems. Domain names only permit one user of a name; there is only one sun.com, which Sun Microsystems registered first. Neither lawyers nor governments can make ten pounds of names fit into a one-pound bag.'

The different nature of domain names and trade marks can lead to commercial, technical and legal problems relating to conflicts between trade marks. If a business owns a trade mark in the UK, can it stop a US company using it as a domain name? This question, and others, will be explored below.

REGISTRATION OF TRADE MARKS

4.7 In the United Kingdom there are three types of registered trade marks, as well as certain protection for unregistered marks and certain well-known[12] marks.[13] First, it is possible to register a mark under the Trade Marks Act 1994,[14] which grants a trade mark only in the United Kingdom; secondly, it is possible to register a Community trade mark[15] under the Community Trade Mark Regulation (No 207/2009) ('the CTM Regulation'),[16] which grants uniform protection across all 28 members of the EU; and finally, it is possible to obtain protection under the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks ('the Madrid Protocol'). The last of these options enables a single application to be made which grants protection in up to 96 countries[17] by way of 94 separate registrations from a single application.[18]

10 Nevertheless, there had been a long-running dispute between the two companies over the right in the name, which was settled in February 2007: see http://news.bbc.co.uk/1/hi/entertainment/6332319.stm.

11 *The Economist*, Letters, 13 July 1996.

12 Protection under art 6*bis* of the Paris Convention (s 56 of the Trade Marks Act 1994).

13 Special protection also exists for other symbols and signs both within and outside the trade mark system. International organisations and states have special protection for their emblems under art 6*ter* of the Paris Convention (which is given effect by ss 57 to 59 of the Trade Marks Act 1994), the Olympic and Paralympic symbols are also given special protection under the Olympic Symbols etc (Protection) Act 1995.

14 This implements Directive 89/104/EEC which has now been codified as Directive 2008/95/EC. There is currently a proposal being considered to revise this codified Directive (as well as the Community Trade Mark Regulation).

15 It is proposed that these will be re-branded as European trade marks as part of the reform package. The Proposals are: COM(2013) 161 final and COM(2013) 162 final.

16 A reform package has been agreed, and at the time of writing is being finalised, which will rename the Community Trade Mark to the European Trade Mark. This chapter will use its current name.

17 As of 31 October 2015.

18 In the UK this is given effect by the Trade Marks (International Registration) Order 2008 (SI 2008/2206).

Whether a mark is registered under the 1994 Act, the CTM Regulation or in accordance with the Madrid Protocol the protection that is granted is the same in scope within the UK and the requirements that the mark must satisfy to be registered are more or less the same.

Signs that can be registered as trade marks

4.8 It is possible for any sign which is capable of graphical representation to be registered as a trade mark[19] provided that the representation is clear, precise, self-contained, easily accessible, intelligible, durable, unequivocal and objective.[20] These requirements will always be met in relation to a word mark, such as a domain name, as it can be written in straight text. Most traditional trade marks can also be represented to this standard; it is only where a mark is unusual (such as smell or sound) that problems arise. However, these unusual marks will not be examined here.[21]

Absolute grounds of refusal

4.9 In addition to the basic requirement that a sign is capable of being graphically represented, there are several other so-called absolute grounds of refusal that lead to an application to register a trade mark being refused. These are, in summary, that the mark is devoid of distinctive character, that it is descriptive, that it has become generic, that it is functional or that it is deceptive or otherwise contrary to public policy.[22] These various grounds will not be examined generally here. Instead this section will look only at the registration using domain names as its working example.

Distinctive and descriptiveness issues

4.10 In general, a trade mark cannot be registered if the relevant public[23] would think that it is devoid of distinctive character.[24] This exclusion is to prevent the registration of a mark which is incapable of fulfilling its essential

19 Trade Marks Act 1994 (TMA), s 1(1); CTM Regulation, art 4.

20 C-273/00 *Sieckmann* [2002] ECR I-11737, [2003] EMTR 37 at para 46. It is part of the reform package that it will be possible to register things which can be contained in digital files (such as sound files or CAD files).

21 See J Mellor *et al*, *Kerly's Law of Trade Marks and Trade Names* (15th edition, Sweet and Maxwell, 2011).

22 TMA 1994, s 3; CTM Regulation, art 7.

23 C-136/02 *Mag Instrument Inc v Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM)* [2004] ECR I-9165, [2005] ETMR 46 at paras 19 and 49; C-218/01 *Henkel KGaA v Deutsches Patent- und Markenamt* [2004] ECR I-1725, [2005] ETMR 45 at para 50. The relevant public is made up of those who might buy the goods or services.

24 TMA, s 3(1)(b); CTM Regulation, art 7(1)(b).

function, namely distinguishing[25] the goods or services of one undertaking from others which have a different origin.[26] In principle, however, even the simplest marks such as a single letter[27] or number[28] may be registered provided they are distinctive.

In addition it is necessary to address whether a mark is descriptive of the goods and services for which the mark is registered.[29] It is not, for example, permissible to register the trade mark COMPUTERS for computers,[30] but it could be registered for bananas. The exclusion from registration of descriptive marks is intended to protect the general[31] (or public)[32] interest so that other traders may use a mark. In considering such an interest it does not matter whether the mark is presently being used descriptively, it is sufficient that it could be used in that way.[33] But the test should not be applied too rigorously as some marks may allude to the function of the goods or services, but in essence are lexical inventions and so cannot be descriptive.[34]

The assessment of whether a mark has acquired distinctive character across the whole of the relevant territory[35] (and whether it remains descriptive) in respect of the goods or services for which registration has been applied for, may take into account the following factors:

(a) the market share held by the mark;

(b) how intensive, geographically widespread, and long-standing use of the mark has been;

(c) the amount invested by the undertaking in promoting the mark;

(d) the proportion of the relevant class of persons who, because of the mark, identify goods as originating from a particular undertaking; and

25 The distinctiveness bar may actually be very low: see C-64/02 *Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM) v Erpo Mobelwerk* [2004] ECR I-10031, [2005] ETMR 58.

26 C-329/02 *SAT.1 Satellitenfernsehen GmbH v Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM)* [2004] ECR I-8317, [2005] ETMR 20 at para 23; C-37/03 *BioID* [2005] ECR I-7975 at para 27.

27 C-265/09 *OHIM* v *BORCO-Marken-Import Matthiesen* [2011] ETMR 4 at para 38.

28 C-51/10 *Agencja Wydawnicza Technopol* [2011] ETMR 34 at para 31.

29 TMA, s 3(1)(c); CTM Regulation, art 7(1)(c).

30 Similarly, Goldfish is descriptive for pets, but not credit cards: see *O2 Holdings Ltd (formerly O2 Ltd) v Hutchison 3G Ltd* [2006] EWHC 534 (Ch); [2006] ETMR 55 at para 71.

31 C-329/02 *SAT.1* [2004] ECR I-8317, [2005] ETMR 20 at para 25.

32 C-191/01 *Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM) v Wm Wrigley Jr Co (DOUBLEMINT)* [2003] ECR I-12447, [2004] ETMR 9 at para 31.

33 *DOUBLEMINT* [2003] ECR I-12447, [2004] ETMR 9 at para 32.

34 C-383/99 *Procter &* Gamble *Co v Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM) (BABY-DRY)* [2001] ECR I-6251, [2002] ETMR 3, paras 43 and 44; but note that this decision is probably the absolute high point of protection and, following later jurisprudence, similar marks may no longer overcome the descriptiveness hurdle.

35 C-108/05 *Bovemij* [2006] ECR I-7605 makes it clear that a mark must have become distinctive across the whole of the UK for a UK mark and across the whole of the EU for a CTM.

(e) statements from chambers of commerce and industry or other trade and professional associations.[36]

Descriptive domain names

4.11 When this approach is put in context it makes more sense. In some industries, it is often better to be listed under one's services than under one's name. For example, it may be more profitable for a chemist to be listed under 'pharmacies' than under his name. It may appear that the same is true for the internet: the domain name, 'flowers.com' may appear to be far more valuable than 'lindasflorist.com'. However, the advantages of such a registration can be greatly overestimated. Most internet users will search the internet using a search engine (such as Google) and searching under 'florist' would bring up both 'flowers.com' and 'lindasflorist.com'.[37] Indeed, there is probably significantly more commercial benefits in being a sponsored link (and so being highlighted at the top of the page) than there is from having a generic web address.

Nevertheless, there is always an advantage from internet users knowing what a website provides without having to access it and so these generic names do provide some commercial benefit. This commercial benefit, however, may not be possible to protect under trade mark law as flowers.com is descriptive of the goods it provides (flowers) and descriptive marks only become registrable where they have become distinctive through use. In other words, it is necessary to show that the mark, although at first blush descriptive, has now become associated in consumers' minds with the relevant business. In contrast, marks like 'lindasflowers.com' are more likely to be distinctive and so could be registered without waiting for it to acquire so-called secondary meaning.

This means that those individuals who are considering acquiring a domain name are advised to use a distinctive name: this has few disadvantages on the web, particularly now search engines are well developed and utilised, but has the obvious advantage of being registrable at the outset.

Registration of 'www' and '.com' etc

4.12 The prevalence of the internet means that many brands only have an online presence. Such businesses may want to register their full domain name as a trade mark to stop others using similar marks (or domain names). In general, at both the Intellectual Property Office and OHIM, it is possible to register trade marks which include the prefix 'www' or with the suffix '.com'/'.co.uk'. However, both this prefix and such suffixes are normally not thought to have any

36 C-108 and 109/97 *Windsurfing Chiemsee Produktions- und Vertriebs GmbH v Boots- und Segelzubehor Walter Huber* [1999] ECR I-2779, [1999] ETMR 585, para 51; also see C-25/05 *August Storck (Storck II)* [2006] ECR I-5719.

37 In fact, a simple Google search using 'florist' generates 63,800,000 hits (as at 31 October 2015).

trade mark significance. A recent example of this issue arose when Getty Images tried to register photos.com, as the court explained:[38]

> '… the word mark PHOTOS.COM, considered as a whole, reproduces the characteristic structure of a second-level domain name ("photos") and a TLD [top level domain] ("com"), separated by a dot. …that mark has no additional features – in particular, graphic features – because the dot is typically used to separate the second level domain from the TLD. Furthermore, the addition of the element ".com" to the word "photos", which is descriptive and devoid of distinctive character, does not render the sign distinctive as a whole …. Accordingly, in the absence of special characteristics peculiar to the sign at issue, the relevant public's perception of that sign will be no different from its perception of the combination of the two words comprising the sign. It follows that … the relevant public will not be able to distinguish the goods and services covered by the trade mark application from goods and services of a different commercial origin. Consequently, the sign is devoid of distinctive character.'

This decision, which was following an established practice. Means that a mark which is not distinctive or descriptive in itself (eg 'flowers' for flowers or 'photos' for photographs) does not cease to be descriptive simply by the addition of 'www' or '.com'. Secondly, when considering infringement or the relative grounds of refusal 'www' or '.com' might be ignored as having no independent significance.[39] This means that 'www.flowers.com' will usually be considered to be identical to 'flowers' or 'flowers.com'.

Nevertheless, some businesses may wish to register as trade marks their actual domain name, prefix, suffix and all. However, there seems little reason to do so as it will give less rather than more protection. This is because registering as a trade mark the name element of the domain name will also protect the name's use within a domain name.

> *Example 4.1*
>
> David Peters Ltd is a one-man company that specialises in repairing old hi-fi equipment. As the company grows in experience, its owner realises that there is a market in repairing old computer equipment for a pre-determined quotation. The company sets up a website on which restored equipment is offered for sale and on which viewers may enter details of their ailing equipment to receive an emailed repair quotation. The domain name for the site is 'www.compair.com'. To provide added protection for this sign, David Peters Ltd may seek a trade mark registration over the word 'compair' in the appropriate classes. Such a registration is normally sufficient to prevent uses by third parties of the mark www.compair.com as well.

38 T-338/11 *Getty Images v OHIM* (21 November 2012) at paras 24 to 28; adopted by the Court of Justice: C-70/13 *Getty Images v OHIM* (12 December 2013) para 25; also see T-117/06 *DeTeMedien v OHIM* (12 December 2007) para 24.

39 Eg *Reed Executive v Reed Business Information* [2004] EWCA Civ 159; [2004] RPC 40, para 36; also see *Compass Publishing BV v Compass Logistics* [2004] EWHC 520; [2004] RPC 41.

Example 4.2

A data recovery company registers the domain name 'data-recovery.co.uk.' It is the only owner of this domain name; it is unique among not only all data recovery companies, but also all domain name owners. This does not mean that the name is capable of distinguishing the services of its owner from any other company. Without more the company will be unable to register a trade mark over the name.

Registering in relation to goods and services

4.13 A trade mark is registered in relation to goods and services and trade mark applicants must indicate on their applications which goods and services in respect of which protection is sought. Accordingly, a trade mark ('flower') which is registered in respect of milk (Class 29) cannot be used to prevent that mark being used by another trader in relation to laundry detergent (Class 3).[40] This means that trade marks are quite different from domain names. A domain name is necessarily unique and so the one person who owns a particular domain name automatically precludes anyone else from using the domain name for whatever goods that second person sells.

Classification

4.14 To assist with both the application for, and searching of, trade marks goods and services are classified in accordance with the Nice Classification.[41] This system is used both by the Intellectual Property Office[42] and the Community Trade Mark Office (OHIM).[43] It has 45 different classes and each class includes a detailed list of goods and services. Practically, there will be few occasions when a registered trade mark proprietor will need to broaden the scope of an existing trade mark registration when beginning to use the name as a domain name. It is wrong to think that because the medium of exploitation is the internet that the trade mark registration needs to be expanded into other classes.

40 Unless the mark has a sufficient reputation to be protected under s 10(3) of the TMA or art 9(1)(c) of the CTM Regulation.

41 The Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks.

42 Trade Marks Rules 2008 (SI 2008/1797), r 7.

43 Commission Regulation (EC) No. 2868/95, r 2.

Example 4.3

Artsake Ltd is a manufacturer of artists' materials within the UK. It has a trade mark registration in Class 16 to reflect the use of its name Artsake in relation to paper, cardboard goods and other artists' materials. It now wishes to expand its business by setting up a website through which customers can place orders. It chooses the domain name 'artsake.co.uk' and is concerned that it will require additional trade mark protection for the domain. It does not; its existing registration will equally protect its domain name in respect of artists' materials sold over the internet.

There may be times where an individual already has a trade mark registration but is providing new goods or services through a website. In this circumstance there may be a reason to broaden the number of classes or specification for which a trade mark is registered. Some websites are, in trade mark terms, still little more than a digital billboard or leaflet. In contrast, true e-commerce solutions which allow the site to obtain information about the viewer and take payment from a user may lead to an increase in the activities provided through a website. An illustration is where the proprietor of a small local newspaper starts to allow and charge for sophisticated searching of its archives from its website. A change in the nature of the business may be taking place. This proprietor should not simply rely on a registration for paper products, but should widen the specification to include the use of computers to search and access data.

Example 4.4

A car manufacturer that uses its trade mark as a domain name decides to make its website more than merely a digital version of its paper brochures. To do this the dealer includes on its website an applet that acts as a route finder: individuals may type in where they are and where they wish to go and the program generates a map of the quickest route. The map also includes the miles per gallon that the dealer's car would use on the same route, so promoting the fuel economy of the car. The business now involves not only the sale of cars but also the provision of a route-finding service. It would be prudent to broaden the trade mark protection to cover these new services accordingly.

Similarly there will be times where the trade mark owner continues to use the trade mark in a slightly different market of goods or services. For example, a travel agent may well have a trade mark registered in classes including class 39 for travel services. If, however, the agent expands its business to include taking bookings over its website, it may want to consider carefully its existing specification on the trade marks register. In this situation it may be wise to ensure its registration covers the provision of travel services by means of a global network.

It is tempting for internet-related firms to apply for a mark in relation to class 38 which relates to, among other things, telecommunication of information. But in fact, registration in this class is only appropriate for infrastructure providers for the internet and those providing the core activities of internet service providers, such as search engines, hosting chat-rooms, email services and so forth.

Jurors are warned that they 'may also be in contempt of court' if they 'use the internet to research details about any cases' they 'hear, along with any other cases listed for trial at the court'. Presumably, this would therefore include searching for social networking profiles or accounts belonging to those connected with the proceedings. In order to reinforce the message, court staff also warn jurors. The warning that court staff read to jurors now explicitly addresses statements made in relation to the internet and via social networking sites and telephones.

The courts' approach to dealing with technology

5.101 Different courts have different systems for dealing with jurors' electronic devices that can connect to the internet, such as mobile phones, laptops, iPads, iPods, and Kindles. In some courts, jurors are permitted to keep these devices with them in the area where they have lunch and sit during breaks in the trial. However, the devices must be switched off in court, and are removed when jurors are reaching a verdict in the case in the jury room. In other courts, jurors' devices are removed from them for the whole time that they are at court. And in other courts, jurors can keep their devices even when reaching a verdict in the jury room. (Reproduced in 'Contempt of Court: Summary for non-specialists', Law Commission Consultation Paper No 209 at paras [147–148].)

CHAPTER SIX

Data and data protection

'And while serious – very serious – the privacy issues we're dealing with today are trivial compared to what's ahead. What are the implications for individual privacy in a world where millions of people are driving internet-enabled cars that have their movements monitored at all times? What happens to privacy for millions of people with internet-enabled pacemakers?'

Lou Gerstner, Chairman & CEO of IBM[1]

'There is an inherent security issue with many of these online exchanges which is often overlooked. Emails are not particularly secure.'

C Davies, Editorial, *Communications Law* (2012) (17), pp 38–39

INTRODUCTION

6.1 An editorial in the *Computer Law & Security Review* notes that '[p]rivacy and data protection issues are never far from the horizon at the moment. There are waves of discussion in this area … and currently that wave is riding high.'[2] The increasing 'centralisation of information through the computerisation of various records has made the right of privacy a fundamental concern'.[3]

Just at the time of finalising this draft, the decision in the *Schrems EU – US Safe Harbor* case has issued.[4] This has been described as one of the most important case decisions that the ECJ/CJEU has ever issued. It affects fundamental right of citizens, trans-Atlantic relations, politics, business, data transfers affecting millions of individuals and some of the biggest multinationals on the planet (as well as thousands of other companies). There are also inter-EU ripples to this case. The immediate question is whether transfers of EU data to the US will

1 eBusiness Conference Expo, New York City, 12 December 2000.
2 Editorial, Saxby, S, *Computer Law & Security Review* (2012) (28), 251–253, at 251.
3 'Personal Data Protection and Privacy', Counsel of Europe, available at http://hub.coe.int/web/coe-portal/what-we-do/rule-of-law/personal-data?dynLink=true&layoutId=35&dlgroupId=10226&fromArticleId=.
4 *Schrems v Commissioner*, ECJ/CJEU. Case C-362/14, referred for a preliminary ruling on 25 July 2014 by the Irish High Court, decision on 6 October 2015. Note also the much commented upon AG Opinion dated 23 September 2015.

have to stop given that the Safe Harbour Agreement has been declared invalid – with no small acknowledgement to the continuing consequences of the Snowden disclosures. (This is discussed in more detail below).

Data protection is important, increasingly topical, and an issue of legally required compliance for all organisations. More importantly it is part of management and organisational best practice. Individuals, employees and customers, expect that their personal data will be respected. They are increasingly aware of their rights. Increasingly they enforce their rights.

Data protection is also increasing in coverage in mainstream media. This is due in part to large numbers of recent data loss and data breach incidents. These have involved the personal data of millions of individuals being lost by commercial organisations but also trusted government entities.

All organisations collect and process personal data. Whether they are big or new start-ups, they need to comply with the data protection regime. Many issues enhance the importance of getting the organisational data protection understanding and compliance right from day one. These include investigations, fines, prosecutions, being ordered to *delete* databases and adverse publicity.

In addition, organisations often fail to realise that data protection compliance is frequently an issue of dual compliance. They need to be looking both *inward* and *outward*. Internally, they have to be data protection compliant in relation to all of their employees' (and contractors') personal data, which traditionally may have related to HR files and employee contracts, but now includes issues of electronic communications, social networking, internet usage, filtering, monitoring, on-site activity, off-site activity, etc.

Separately, organisations have to be concerned about other sets of personal data, such as those relating to persons outside of the organisation (eg customers, prospects, etc). Comprehensive data protection compliance is also required. The consequences are significant for non-compliance.

Substantial fines have been imposed in a number of recent cases. In some instances also, organisations have been ordered to delete their databases. In a new technology start-up situation, this can be the company's most valuable asset.

Until recently the issue of data loss was a small story. More recently, however, the loss of personal data files of millions of individuals in the UK – including from official and non-governmental sources – makes UK data loss a front page issue. There is increased scrutiny from the ICO, and others, and new regulation is forthcoming.

In the UK and elsewhere there are enhanced obligations to report all data losses; as well as discussion to have enhanced financial penalties and in some instances personal director responsibility for data loss. The need for compliance is now a boardroom issue and an issue of corporate compliance. Proactive and complete data protection compliance is also a matter of good corporate governance, brand loyalty and a means to ensuring user and customer goodwill.

The frequency and scale of recent breaches of security, such as Sony Playstation (70 million individuals' personal data[5] in one instance and 25 million

5 See, for example, Martin, G, 'Sony Data Loss Biggest Ever', *Boston Herald*, 27 April 2011, available at http://bostonherald.com/business/technology/general/view/2011_0427sony_data_loss_biggest_ever.

in another[6]), TalkTalk, Vodafone, etc, make the topicality and importance of data security compliance for personal data ever more important. (Sony is also central in issues surrounding the hacking of its systems leading to it to pulling the premier of its film *The Interview*, apparently under cyber threat of further retaliation for the film. This is a new escalation in the dangers posed of hacking and its legal and policy consequences.) The largest UK data loss appears to be from the loss by HM Revenue and Customs of discs with the names, dates of birth, bank and address details for 25 million UK individuals.[7]

There are many new UK cases involving substantial fines for data protection breaches. The Brighton and Sussex University Hospitals NHS Trust had a fine of £325,000 imposed by the ICO in relation a data loss incident.[8] Zurich Insurance was fined £2.3 million for losing data in relation to 46,000 individual customers.[9]

National data protection authorities are increasingly proactive and undertake audits of data protection compliance frameworks, as well as incidents of breaches. Facebook internationally has been audited by one of the EU data protection authorities.[10] The ICO is also involved in dealing with personal data issues relating to the phone hacking scandal which is also the separate subject of the Leveson Inquiry.[11] This ICO investigation is called Operation Motorman.[12]

COMMERCIAL IMPERATIVES/PERSONAL PERSPECTIVES

6.2 Businesses demand that their digital presences, including websites, collect and analyse personal data. They collect it, not only to ensure that simple things are performed correctly, such as delivering goods to the right address and managing subscriptions. They also collect to predict their customers' needs. The more sophisticated collect personal data to sell or rent to other businesses to help them predict their customers' needs. In short, businesses view personal data as a critical asset.

6 See, for example, Arthur, C, 'Sony Suffers Second Data Breach with Theft of 25m More User Details', *Guardian*, 3 May 2011, available at www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

7 See, for example, 'Brown Apologises for Record Loss, Prime Minister Gordon Brown has said he 'Profoundly Regrets' the Loss of 25 Million Child Benefit Records', BBC, 21 November 2007, available at http://news.bbc.co.uk/2/hi/7104945.stm.

8 See, for example, 'Largest Ever Fine for Data Loss Highlights Need for Audited Data Wiping', *ReturnOnIt*, available at www.returnonit.co.uk/largest-ever-fine-for-data-loss-highlights-need-for-audited-data-wiping.php.

9 See, for example, Oates, J, 'UK Insurer Hit with Biggest Ever Data Loss Fine', *The Register*, 24 August 2010, available at www.theregister.co.uk/2010/08/24/data_loss_fine/. This was imposed by the Financial Services Authority (FSA).

10 The audit relates to Facebook internationally, outside of the US and Canada. See first stage of the audit report, of 21 December 2011 at http://dataprotection.ie/viewdoc.asp?m=&fn=/documents/Facebook%20Report/final%20report/report.pdf. It is entitled *Facebook Ireland Limited, Report of Audit*, and was conducted by the Irish Data Protection Commissioner's Office. Note also complaints and access requests referred to at Europe Against Facebook, available at http://europe-v-facebook.org/EN/en.html.

11 Available at www.levesoninquiry.org.uk/.

12 Footnote: Available at www.levesoninquiry.org.uk/.

For the customers and other individuals whose information comprises this asset, there is an increasing expectation that businesses will use their data responsibly; that they can retain some control over how it is used and not, for example, have their email inboxes inundated with unwanted marketing communications or their personal details sold or disclosed indiscriminately. In the UK, the Information Commissioner and data protection regime are positioned to ensure that businesses respect the individuals whose data is being harvested, and uphold their rights.

But in an industry where the valuable data of individuals may be collected in ever-increasing number of ways, in ever-more exacting detail, on an ever-increasing scale, continuously, combined and cross-referenced, traded and exchanged outside of the UK in an instant, and spam sent from anonymous sources located in other jurisdictions, such protections have immediately apparent limitations.

From another angle, personal information is valuable not only to the businesses who collect and trade in it, but is also an essential source of evidence for law enforcement and other agencies wishing to build up profiles and details of a suspect's communications, tastes, movements, behaviour and transactions. It increasingly also features in civil law, family law and employment tribunal related cases. Any internet business which may collect or have access to such data therefore becomes a significant law enforcement and investigation resource, and may expect requests for disclosure of information. One of the most interesting and potentially important cases in relation to law enforcement access to personal data held by technology companies involved a case in the US where Microsoft is appealing a non-judicial request for data held in a data centre in Ireland which it says is outside of the normal international protocols and procedures for such access. Various technology companies are supporting Microsoft. The Irish Minister for Data Protection has raised concerns that normal international procedures are not being followed. Various industry commentators feel that if Microsoft were to lose the appeal, there would be a grave adverse affect on the US Cloud services industry.[13] How do these businesses know how to balance their obligations to the data subjects against requests from other regulatory or enforcement bodies?

As criminals become ever more technically savvy, but also dependent on internet communications, and concerns grow about international terrorism and crime, it is clear that the importance and value of such data, and therefore the number of disclosure requests, will only increase. In the UK and throughout Europe, legislation has been developed to put in place a procedural framework for handling and responding to such requests, safeguarding fundamental rights and clarifying when disclosures may be made without fear of legal action. In addition, steps have also been made to require that internet service providers retain minimum communications data precisely so that it can be available for law enforcement purposes.

13 See, for example, J O'Connor, 'The Microsoft Warrant Case: Not Just an Irish Issue', *Computers and Law*, Society of Computers and Law, 7 October 2014.

THE LEGISLATIVE LANDSCAPE

6.3 UK legislation on data breaks down into three interrelated areas. First, the basic data regime which upholds individuals' rights in respect of the processing of their data by imposing obligations on those who control it. A second imposes specific obligations on how data may be used for electronic marketing and other value added purposes. The third sets the parameters in which data may be made available for law enforcement purposes. All of these have been introduced to enact European Directives.

The Data Protection Act 1998

6.4 The Data Protection Act 1998 replaces the Data Protection Act 1984. The new legislation was brought into force following a review of data protection across Europe by means of the Second European Convention on Data Protection and the 1995 Data Protection Directive. The new regime introduced new rights and powers of enforcement, prohibitions on transfers of data outside of the EEA to countries with 'inadequate' data protection regimes, and a strengthening of security obligations.

The Act is the starting point for consideration of an internet or website provider's obligations in respect of their customers' and users' personal data. Since its introduction the Information Commissioner's Office (ICO) (which enforces the data protection and freedom of information regimes in the UK) (and which has equivalent national data protection authorities in the other EU member states) also publishes various guidance and codes of practice clarifying the scope of the Act's obligations on those with control over the processing of personal data. (The EU Article 29 Working Party on data protection, which comprises members of the EU national data protection authorities, including the ICO, also publishes sector-specific data protection guidance.) Although many enforcement actions have tended to be at an informal level, the last few years have revealed that increasingly significant fines and prosecutions are arising in the event of data protection breached. This also occurs in the state/official sector as well as the commercial sector. Individuals are also becoming more alert to their rights. The press is also more ready to publicise stories of security breaches and mismanagement of data, as concerns about fraud and identity theft have grown. In parallel, there are now indications that more robust and proactive enforcement may follow. There is an increasing emphasis on director liability issues and board responsibility for data protection compliance.

The Privacy and Electronic Communications (EC Directive) Regulations 2003

6.5 Although the Data Protection Act 1998 contains basic rights and protections for data subjects, European Directives have developed more detailed rules in respect of the sending of unsolicited direct marketing messages using

publicly available telecommunications services (eg mobile or fixed telephone, fax and email). In the UK, this legislation was first implemented in March 2000 by way of the Telecommunications (Data Protection and Privacy) Regulations 1999 implementing European Telecoms Directive 97/66/EC. The Directive was implemented differently across Europe, however, resulting in uncertainties as to key definitions and potential bars to harmonisation. A new Directive 2002/58/EC on privacy and electronic communications followed and has been implemented in the UK in the guise of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

These Regulations contain clearer rules concerning direct marketing via electronic means, specifically as relates to email or 'spam' marketing, but also regarding the use of website cookies and other tracking devices such as web beacons to harvest users' personal data; and the extent to which users' traffic and billing data may be used after a communication has ended.

The Regulation of Investigatory Powers Act 2000

6.6 The Regulation of Investigatory Powers Act 2000 (best known by its acronym 'RIPA') received Royal Assent on 28 July 2000. Very lengthy and technical in nature, RIPA covers five specific areas. First, it contains prohibitions on the interception of communications in the course of their transmission and defines the circumstances in which this may be authorised and subscriber data may be made available for law enforcement purposes. Second, it contains rules relating to surveillance, proscribing techniques that may be used with a view to safeguarding the public from unnecessary invasions of their privacy. These two parts will be of most interest to those providers or internet networks and services. The latter parts of RIPA cover encryption of data, judicial oversight and the establishment of a tribunal providing redress against those exceeding their powers under RIPA.

Under RIPA sits various secondary legislation. The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 provides for obligations which the Secretary of State may impose on service providers to establish and maintain system capability for interception in the event that this is required under RIPA. The Order only applies to providers of public telecommunications services offered to more than 10,000 persons in the UK.

The other key secondary legislation is the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 which authorises specified interceptions carried out by persons in the course of their business for the purposes relevant to that business (such as monitoring staff email and general running of the system) and using that business's telecommunication system which would otherwise be unlawful under RIPA.

This all needs to be read in conjunction with: (a) the post-Snowden environment and related developments; and (b) the *Digital Rights Ireland* Court of Justice case (*DRI*) (see below) and related cases. Even in the US, the Patriot Act fell by virtue of non-renewal.[14]

14 The US Senate a week later in June 2015 did pass the Freedom Act, which is meant to curb some official data collections and data retention.

Post the *DRI* case, the government rushed through the Data Retention and Investigatory Powers Act or DRIPA[15] to cater for data retention issues on a short-term basis. However, this was also challenged.

Two MPs (David Davis and Tom Watson), successfully challenged the Data Retention and Investigatory Powers Act 2014 (DRIPA) in the High Court. The court held that sections 1 and 2 of DRIPA breached rights to respect for private life and communications and to the protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The decision gives the Government until March 2016 to rectify the DRIPA problems.

The most recent Queen's speech has also promised a 'snooper's charter' which would replace DRIPA.[16] No doubt argument, debate and research will ensue.[17] It remains to be seen how challenge to DRIPA may transpire, and how courts and policy makers will react. This remains, if anything, a contentious issue.

Anti-Terrorism, Crime and Security Act 2001

6.7 The Anti-Terrorism, Crime and Security Act 2001, introduced following the 9/11 terrorist attacks in the US, provides government with further powers to counter threats to the UK. The provisions of the Act of specific interest to internet providers concern the rights granted to government departments and agencies to require the disclosure of data for national security purposes. The Act itself contains little detail, but Part 11 allows for the development of a voluntary statutory code for retention and contains reserve powers to enable further powers to be brought in if needed.

A Code of Practice for voluntary retention of communications data was drawn up and came into force on 5 December 2003, despite reservations from the internet service provider community. It seeks to encourage service providers to retain types of data which they already hold (as opposed to requiring the restructuring of systems to enable retention of new types of data) for specified periods ranging from four days to 12 months depending on the type of data.

As indicated above in relation to RIPA, this also needs to be read in conjunction with (a) the post-Snowden environment and related developments; and (b) the *Digital Rights Ireland* (*DRI*) Court of Justice and related cases.

The most recent Queen's speech and referred to legislation may also be relevant.[18]

Readers are advised to consult specialist texts in relation to the unfolding issues regarding if and how the RIPA/DRIPA/Data Retention Directive may be

15 See www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014.

16 See T Whitehead, 'Google and Whatsapp will be forced to hand messages to MI5,' Telegraph, 27 May 2015, available at www.telegraph.co.uk/news/politics/queens-speech/11634567/Google-and-Whatsapp-will-be-forced-to-hand-messages-to-MI5.html.

17 See generally TJ McIntyre, 'Cybercrime – Towards a Research Agenda' in Healy, Hamilton, Daly and Butler (eds), *Routledge Handbook of Irish Criminology* (Routledge, 2015).

18 See T Whitehead, 'Google and Whatsapp will be forced to hand messages to MI5', Telegraph, 27 May 2015, available at www.telegraph.co.uk/news/politics/queens-speech/11634567/Google-and-Whatsapp-will-be-forced-to-hand-messages-to-MI5.html.

replaced in light of being undermined by the Court of Justice in the *DRI* (and other) cases and challenges, including in the UK.

Directive 2006/24/EC on data retention

6.8 Data retention is sometimes a controversial topic. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks is the final key statute. This requires member states to implement measures to require the retention of certain data so that it can be made available to law enforcement authorities and government agencies for the investigation and detection of crime. This is a step forward from the voluntary Code of Practice under the Anti-Terrorism Act discussed above, to provide a compulsory and harmonised minimum level of data that must be retained by communications providers.

The regulation for retention of telephone data is subject to political and legal change, as well as debate.

As mentioned above, data retention is sometimes controversial and has attracted criticism such as on civil liberties, secrecy, overreach, etc. There have been a number of challenges to the Directive and to national measures regarding data retention. In the most significant case, *Digital Rights Ireland*, The Court of Justice struck down the Directive as, *inter alia*, being over-broad.[19] The Directive was held to breach arts 7 and 8 of the European Charter of Fundamental Rights.

It is possible that a new European data protection measure will be drafted in light of the decision. Queries arise in relation to the legality or necessity of data retention by telecoms companies presently. It is understood that at least one telecoms company has decided to delete such data on the basis that there is currently no legal basis to (have to) store the same. Some governments may perceive the need for national emergency legislation. Others may await the new EU data retention measure to replace the Directive which has been struck down. On a general note it should not be underestimated what backdrop effect the Snowden revelations may have had on the decision. The UK government feels the need for such emergency data retention legislation.[20]

DATA PROTECTION

6.9 Before investigating the application of the Data Protection Act 1998 to the internet, it is vital to set out the main aspects to the legislation. The Act is particularly definition-based: to appreciate the responsibilities of a data user

19 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* Judgment of 8 April 2014. *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung (C-594/12) and others*. Available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-293/12.

20 See, for example, 'Emergency phone and internet data laws to be passed', BBC, 10 July 2014, available at www.bbc.com/news/uk-politics-28237111.

one must appreciate a great number of separate concepts: data, personal data, relevant filing system, processing of data, data subject and recipient. For ease of understanding, therefore, this section attempts to simplify the legislation by referring to these issues. This section describes each of these issues with specific internet examples; the following sections consider the application of these issues to commonplace e-commerce transactions and activities on the internet.

Personal data

Data

6.10 The Act applies only to personal data and those dealing with it. Assessing whether information is personal data is the starting point for all data protection questions. The word, 'data', is circularly defined with reference to further defined terms which themselves refer to 'data.'[21]

This wide definition is:

> 'information which:
>
> (a) is being processed by means of equipment operating automatically in response given for that purpose;
>
> (b) is recorded with the intention that it should be processed by means of such equipment;
>
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
>
> (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by s 68 [including health records, education records and accessible public records].'

In this way 'data' encapsulates information processed by equipment, either automatically or that is intended to later be processed by equipment. One example would therefore be information collected from individuals by way of physical paper forms which are to be later transferred into computer files. 'Equipment' is not defined in the Act and is deliberately technology-neutral. A computer would be an obvious example of equipment caught by both (a) and (b) above (others would include cameras, dictaphones, PDAs, etc). Therefore, any website or internet server is unlikely to be caught by section (a).[22]

Although unlikely to be relevant to the internet, the definition also captures non-digitally processed data which remains in manual files, but only if these

21 Data Protection Act 1998, s 1(1). This definition is not drawn from the body of the Directive but rather its preamble.

22 The case of *Smith v Lloyds TSB Bank* [2005] EWHC 246 held that the issue of whether information was personal data had to be answered at the time of the request. At that time Lloyds did not hold any information about Smith wholly or partly on automatic equipment. The reference to and definition of a relevant filing system in s 1(1) would be meaningless if any documents capable of being converted into a digital format were to be treated as if they were in a computer database.

form a part of a 'relevant filing system'. 'Relevant filing system' is defined by s 1(1) as:

> 'any set of information relating to individuals to the extent that although the information is not processed by means of equipment generating automatically in response to instructions given for that purpose, the set is structured as by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.'

This is a possible qualification, highlighted in the case of *Durant v Financial Services Authority*.[23] This means that unsophisticated records such as those which are structured purely by date rather than by name, for example, are unlikely to be caught. Unfortunately for internet providers, although relevant filing system is not stated as applying solely to manual records, the fact that computer records and internet files will be caught by limb (a) of the definition of data means that this caveat is not available. Although a digital record may be difficult to search against an individual, a controller will not clearly be able to rely on this in the same way as the Financial Services Authority did in relation to Mr Durant's paper files. This case has, however, been criticised and is distanced in discussions by other Data Protection Authorities. On a separate note, the Leveson Inquiry notes that judges (as well as others) need to become more familiar with data protection law.

Example 6.1

RemCom gathers salary data from recruitment agents to allow prospective employees to gauge their potential remuneration package in a given job. When an employee gains employment they are encouraged to feed back into RemCom their new salary and benefits package. Even though some of this information is taken from the happy employees by telephone operators, before it is inputted into RemCom's database, it will be classified as data.

Personal data

6.11 The word 'personal' refers to the data:[24]

> 'which relate 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 and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.'

While this definition is fundamental to whether or not one has data protection obligations, personal data may not be fundamental to a successful internet or e-commerce initiative.

23 [2003] EWCA Civ 1746.
24 Data Protection Act 1998, s 1(1).

Example 6.2

An individual repeatedly visits a website and always downloads from it the latest screensaver of a particularly attractive tennis star. Because the individual has entered data into an on-screen form, the website 'knows' four items of data about the individual. The individual is male, between 25 and 35 years of age, earns over £45,000 a year and likes tennis. Each time the individual visits the site, the site confirms it is him by placing on his computer a small file containing a unique identifier. The site, therefore, 'knows' what he looks at, what he downloads, how often he visits etc. All this data is useful and helps the site target the individual with new relevant screensavers when he visits. Without more, however, the site holds no personal data. The Act is not applicable therefore but the Privacy and Electronic Communications (EC Directive) Regulations 2003, are.

This technique of using 'non-personal' data has led e-commerce businesses to explore whether or not they can entirely avoid the obligations of the Act.[25] To consider this avoidance of the Act, one first needs to appreciate the scope, and purposive interpretation, of the definition. Key elements are as follows.

Relate to an individual

6.12 Previously it was thought that the Act concerns the data rather than the individual to whom it relates. This view is rebutted by the Court of Appeal's ruling in *Durant v Financial Services Authority*.[26] The court in this case focused on when data can be said to 'relate to an individual'. The court held that data could only be said to be 'personal' if it 'is information that affects [a person's] privacy, whether in his personal, or family life, business or professional capacity'. It went on to give two ways in which this might be determined. The first was whether or not the information is 'biographical in a significant sense', meaning that it goes beyond just mere recording of data to require some kind of personal connotation. The second appears to go further still, being that the data should have the individual as its focus rather than some other individual.

The Information Commissioner has clarified this interpretation as meaning that the simple fact that 'an individual is referred to in data does not make the information personal data about that individual unless it affects their privacy'.[27] Commentators and national Data Protection Authorities may not fully endorse the perhaps restrictive view of *Durant*.

Even if the decision in relation to relevant filing systems does not help those holding internet or other computer records (see **6.10** above), this part of the judgment does. Indeed the court specifically stated that 'not all information retrieved from a computer search against an individual's name or unique identifier, constitutes personal data'.[28] Obvious examples may include, in certain

25 Of course, companies still need to ensure they comply with the Act in relation to their other personal data: personnel, suppliers, contacts, etc.
26 [2003] EWCA Civ 1746.
27 'The "Durant" case and its impact on the interpretation of the Data Protection Act 1998', guidance note of the Information Commissioner issued in February 2006.
28 Ibid.

circumstances, an email which a person is simply cc'd in on. However, a record which shows what a person bought, their payment records or address would do. Most website transaction records and even log records which show what pages and services an individual was using are still likely to be caught therefore. The *Durant* ruling forces one to analyse what personal data is and is thereby caught by the Act. Rather than assuming that any data which can be related back to an individual is, one must assess whether the data does actually relate to and affect an individual. A cautious approach to overreliance on *Durant* is advised however.

A common scenario concerns an email address. Most email addresses incorporate the actual name of an individual and therefore relate to that individual, but this does not mean that it is automatically personal data. If I am simply cc'd in on a chain of emails discussing someone else, then it may be (in the *Durant* view) that my email in that context or the email itself does not constitute personal data. One can see from just this example that the analysis required varies on a case-by-case basis and demands some thought. In most cases controllers will want and need to err on the side of caution in discharging many of their obligations, treating emails with care. However, when it comes to data subject to access requests (as discussed later), controllers may wish to consider this more closely, rather than simply handing over and redacting quantities of information and material.

The *Durant* ruling has been followed in the case of *Ezsias v Welsh Ministers*,[29] concerning information to be provided pursuant to a data subject access request. The High Court held that only information relating to Mr Ezsias, as opposed to that relating to, say, his complaints, had to be provided. Further, to use the provisions of the Act to seek disclosure of documents generated as the result of the applicant's own complaint, in order to further a legal claim of the applicant against a third party is a legal abuse.

Many national data protection authorities would not necessarily take the perceived restrictive view of the *Durant* case. The Court of Justice case of *Commission of the European Communities v The Bavarian Lager Co Ltd*, annulled a Commission decision rejecting an application for access to the full minutes of the meeting, containing all of the names,[30] which is also arguably more in line with interpretations of what is personal data than the *Durant* view.[31] One view may be that a possibly restrictive *Durant* interpretation has received a more mainstream interpretation in the *Bavarian* case. Records of employees' working

29 [2007] All ER(D) 65.

30 *Commission of the European Communities v The Bavarian Lager Co Ltd*, Case C-28/08 P. Note also another ECJ/CJEU case which held that 'Article 2(a) of Directive 95/46/EC … must be interpreted as meaning that the data relating to an applicant for a residence permit contained in an administrative document, such as the "minute" at issue in the main proceedings, setting out the grounds that the case officer puts forward in support of the draft decision … and, where relevant, the data in the legal analysis contained in that document, are "personal data"'. In *Joined Cases C-141/12 and C-372/12 YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M, S*, 17 July 2014.

31 In relation to redacted and bombardised access disclosures, see for example, *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47. Also see *Webster and others v the Governors of the Ridgway Foundation School* [2009] EWHC 1140 (QB).

time is personal data.[32] In the *Halford* case, where an employee's UK telephone calls relating to a discrimination case were being recorded, the ECHR held, *inter alia*, that art 8 of the Convention is applicable to complaints concerning both the office and the home telephones; and that that there has been a violation of art 8 in relation to calls made on the applicant's office telephones.[33] The author JK Rowling was concerned to take a case under privacy and personal data grounds in relation to surreptitious photographs taken by certain media of her children.[34] The *Von Hannover* case also relates to protection from certain types of media photography.[35] Recently, the scope of the so-called (individual processing) or household exemption to the ambit of the data protection regime has been considered in the context of CCTV footage. The Court of Justice held that 'the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity' within the exception to applicability.[36]

Living individual

6.13 As long as the individual is living and is not a body corporate, the Act can apply. This includes all individuals, whether resident abroad or of foreign nationality.

> *Example 6.3*
>
> A foreign national enters his personal details into an online form required to access a UK newspaper's website. The individual is now concerned that these personal data are being misused. All things being equal, he has rights under the Act to prevent this misuse because he is a living individual and the data held are personal. The individual's nationality is largely irrelevant to the newspaper's obligations.

The definitions of personal data in both the Act and Directive refer to 'person' and 'individual' and not 'people' and 'individuals'. A question therefore arises

32 See *Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)*, ECJ/CJEU Case C-342/12, 30 May 2013.

33 *Halford v UK Halford v UK*, ECHR (1997), IRLR 471 (1997) 24 EHRR 523. See also *Copland v The United Kingdom*, ECHR (Application no 62617/00) 3 April 2007.

34 See *Murray v Big Pictures (UK) Ltd* (CA) [2008] EWCA Civ 446; [2008] 3 WLR 1360; [2008] EMLR 399, [2008] EHRR 736, [2008] 2 FLR 599, [2008] HRLR 33, [2008] UKHRR 736. Another example of surreptitious photographs were certain holiday pictures taken of Kate Middleton in what was expected to be a private setting.

35 The ECHR held that there was a breach of art 8 of the Convention. *Von Hannover v Germany (No 1)* ECHR (2004), (application no 59320/00), [2005] 40 EHRR 1. Note also later case of *Springer and Von Hannover v Germany (Von Hannover No 2)*, 07.02.12 [2012] EMLR 16. Also note *Axel Springer AG v Germany* (application no 39954/08) relating to the issue of national law.

36 *František Ryneš v Úřad pro ochranu osobních údajů*, ECJ/CJEU, Case C-212/13, 11 December 2014.

whether or not the Act applies to processed data about 'joint' individuals. Certainly, joint bank account holders are likely to be considered each as an individual under the Act, as are joint tenants of property.

Example 6.4

A well-known department store establishes an online wedding site for couples to create a 'micro-site' before their happy day. As well as displaying directions to the venue and a ceremony of service, the micro-site also provides the chance for guests to make purchases from the couple's gift list. Together with their address and wedding day, the department store does possess data relating to an individual.

However, there is at least academic and the Article 29 Working Party discussion on whether some data protection interests should survive death.[37]

Possession of other information

6.14 The definition of 'personal' data refers to identification in conjunction with other information in possession or likely to come into the possession of the data controller.[38] The Directive's recital 26 illustrates the likely width of 'possession'. It states:

> 'To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person.'

It follows that it is still possible to have 'possession' of data permitting identification for the purposes of the Act, even if one does not actually have physical possession of it. When assessing whether or not one is processing personal data, one must therefore examine data which is publicly available (which would 'confirm' the identity of the individual) and data available from a third party under contract or other relationship. This ties in closely with scenarios in which a company may believe that its data is not caught because it is anonymous. Since the key to decrypt or encode the data may be available, the data is still caught.

Another common example concerns IP addresses. An IP in itself appears as a number. This identifies a computer or log on point, rather than an individual. However, if a controller holds account details for an individual including their IP address and uses an IP address to collect further information (eg tracking which pages are read on a website), the information so collected becomes personal data since it can be related back to the individual and says something about them. This is the case even if the IP collected information and the account data is held in separate files. The fact that it could be linked causes the problem.

37 See, for example, Article 29 Working Party, Opinion No 4/2007 on the concept of personal data (2007) WP 136, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. See discussion at 22.

38 Data Protection Act 1998, s 1(3).

Example 6.5

SecuriFirst and Last is a security firm which generates digital 'safes' for people who wish to store digital data off their own hard drives. To do so, one must provide one's first name, date and place of birth to SecuriFirst and Last. One pays for the safe through a third party which takes one's full name and residential address. This third party then provides a password to enable 'unlocking' of the safe. The third party clearly can identify each customer using information in its possession; SecuriFirst and Last also is likely to come into possession of this information because of its relationship with the third party.

Opinions on individuals

6.15 The final test to establish whether data is personal data is to ascertain the nature of the data: if the data is an expression of opinion or indication of intention about the individual, then the data can be personal.

The definition also includes an intention being expressed by a third party. For this reason, repeating the intention of another with respect to a living individual will still fall within the definition; the data may still be personal.

Anonymous data

6.16 The Data Protection Directive explicitly states that: 'the principles of protection shall not apply to data rendered anonymous'.[39] In addition, the Act refers only to living individuals who can be identified from the data processed. This has led many website operators and e-commerce businesses to seek to force (technically or legally) their data into being anonymous and so avoid the regulation of the Act. This is easier said than done. This is particularly so in the era of profiling, connecting information data and big data.

When businesses talk of 'anonymised', 'aggregated', 'generic', or even 'neutered' data, they may be referring to a number of situations. Common explanations of anonymous data include:

1. 'My business cannot identify living individuals from information we have in our possession. If we wanted to obtain extra information to do so, we could.' This business only possesses anonymised information. It will still be classified as personal data because reasonable enquiries would enable them to turn the anonymised data into identifying data.

2. 'My business cannot identify living individuals from information we have in our possession. We have come to an arrangement with a third party; they hold the personal data, we merely hold a unique identification number which allows them to resolve the identities.' This business only possesses anonymised information. Unless their contract with the third party is unambiguous, it is likely that their relationship will allow them to resolve

39 Recital 26.