CHAPTER 2

Privacy Rights Under The Human Rights Act 1998 And Remedies For The Misuse Of Private Information

INTRODUCTION

Since the implementation of the Human Rights Act 1998 (HRA) the law has developed to provide remedies where the private information of individuals has been or is threatened to be misused. This is a right independent of those guaranteed by the Data Protection Act 1998 (DPA) and, although the information covered by the remedy is not as broad as that covered by the DPA, is a significant addition to the protection of privacy in the UK. The essence of the development of the law in this area was captured by Lord Hoffman in 2004 in *Campbell v MGN Ltd*,[1] explaining where the law stood as well as looking forward to the questions yet to be addressed. 2–01

> "In recent years there have been two developments of the law of confidence....One has been an acknowledgement of the artificiality of distinguishing between confidential information obtained through the violation of a confidential relationship and similar information obtained in some other way. The second.....has been the acceptance of the privacy of personal information as something worthy of protection in its own right ...
>
> "What human rights law has done is to identify private information as something worth protecting as an aspect of human autonomy and dignity. And this recognition has raised inescapably the question of why it should be worth protecting against the state but not against a private person.... I can see no logical ground for saying that a person should have less protection against a private individual than he would have against the state for the publication of personal information for which there is no justification ...
>
> "The result of these developments has been a shift in the centre of gravity of the action for breaches of confidence when it is used as a remedy for the unjustified publication of personal information ... Instead of the cause of action being based upon the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity—the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people ...
>
> "These changes have implications for the future development of the law. They must influence the approach of the courts to the kind of information which is regarded as entitled to protection, the extent and form of publication which attracts a remedy and the circumstances in which publication can be justified."

[1] [2004] UKHL 22.

As foreseen by Lord Hoffman, over the last eight years the courts have been asked to consider the kind of information which requires protection as well as rights to anonymity, prior notice of intended publication and how the balance between individual privacy and public interest in publication should be achieved. The new rights to take action are welcome. It has to be recognised, however, that cases have been fought tooth and nail by some sections of the press and one senior judge has been subject to personal criticism as a result of his judgments.[2] At the same time the irrelevance of the court system for most ordinary people has been thrown into focus by the revelations about the behaviour of parts of the tabloid press. At the time of writing[3] the question of how journalists can be restrained from making unjustified intrusions into privacy is being canvassed in the Leveson Enquiry into Press Standards.

This chapter describes the development of the law of confidence in the UK, the effect of the HRA, case law from the European Court of Human Rights (ECtHR) at Strasbourg on informational privacy under art.8 of the European Convention on Human Rights (the Convention), the impact of Convention Rights on the interpretation of the data protection directives, and outlines the development of the tort of misuse of private information in the case law in the UK since the implementation of the HRA. It includes an outline of the relevance of art.10, but material on press regulation and some more detailed material will be found in Ch.17 on the exemptions for journalistic and literary purposes. It is recommended that these two chapters should be read together.

2–02 SUMMARY OF MAIN POINTS

(a) There is no over-arching cause of action in English law for breach of privacy.

b) The misuse of private information will give rise to a remedy before the courts in certain circumstances. This is equally applicable between private parties. In applying this right the courts will apply art.8 of the Convention rights.

c) Personal information can be protected where the person had a reasonable expectation of privacy in respect of the information. There is no need for the parties to have been in a prior relationship.

d) The categories of the information that may be protected are not closed but the essence is that the action protects the dignity and autonomy of the individual. Thus the information may be related to behaviour in public places or information which is known to a limited number of people. Those who are in the public eye or have a public role are as entitled to have their privacy protected as anyone else. Particular care is required to protect the privacy of children and it is recognised that photographs are more intrusive that mere words.

[2] The editor of the *Daily Mail*, Paul Dacre, giving the opening speech at the Society of Editors Conference in 2008 criticised the role of Lord Justice Eady in setting significant precedents in privacy cases.

[3] May 2012.

e) The right of free speech is an important human right but it is not paramount. Neither privacy nor freedom of speech are absolute rights, nor is one superior to the other.

f) Where the person who wishes to publish personal information which would affect the privacy of another invokes the right of freedom of speech, the courts must carry out a balancing act between the two rights set out in arts 8 and 10, taking into account the justification for interfering with or restricting each right and applying considerations of proportionality.

g) The right of free speech is one of the most important rights in a democracy and must be fiercely guarded but not all speech has the same value. The right to free political speech is much more important than the right to repeat trivial gossip.

h) Where the disclosure is justified in the public interest, for example to "set the record straight", then it must still be proportionate.

i) There is no legal right to prior notice of intended publication of private information.

j) An interim injunction should not be granted unless the court is satisfied that the claimant is likely to obtain an injunction following trial.

k) Exemplary damages are not recoverable in an action for misuse of private information.

l) In some circumstances the applicant may be entitled to anonymity but the circumstances in which a privacy case will remain unreported ("a super injunction") will be extremely limited and such orders will generally be time-limited.

m) It is no defence to assert that the information is false or inaccurate.

COMMERCIAL EXPLOITATION IMAGE

2–03 The law of the UK does not provide a statutory right to prevent the commercial exploitation of the image of the individual. However it appears that the courts will now afford protection for commercial interests in images. Thus photographs resulting from a photoshoot which had been opened to fans to view were protected on the grounds of confidentiality in *Creation Records v News Group Newspapers Ltd*.[4] In making an order to restrain the publication of pictures of a house purchased by a celebrity couple, there was an acknowledgement that the couple had an interest, not only in protecting their privacy, but in the possibility of selling an "exclusive" set of pictures of the property to a magazine.[5]

In some cases where the individual has a commercial interest in the image which the individual could legitimately exploit and which has been unfairly exploited by another party without permission, protection has been provided by the tort of passing off. This is clearly a remedy to protect a commercial interest.

[4] [1997] E.M.L.R. 444. Case concerned the Oasis photoshoot for a record album cover. A Rolls Royce was put into a swimming pool. Fans were allowed to watch but when one took a photograph and offered it for publication in a newspaper the record company succeeded in restraining the use of the photograph.

[5] *Beckham v MGN* Unreported June 28, 2001, QBD.

Actions can also be taken for breach of confidence where there is a clear obligation of confidence to protect private pictures which have a commercial value.

In *Douglas v Hello! Ltd*,[6] it was accepted that a couple were entitled to protect the exclusive photographic rights to official pictures of their celebrity wedding, to which over 300 guest had been invited, to the extent that they had a legitimate commercial interest in the exploitation of the pictures. In the Court of Appeal it was held that this was a species of property right that could not be passed on to another and hence *OK!* were unable to benefit. However, on appeal to the House of Lords *OK!* succeeded in establishing that the arrangements entered into for the security of the wedding had created a form of confidentiality which protected its interests as well as that of the protagonists and were successful in their action for breach of confidentiality by *Hello!* magazine.

In Edmund Irvine Tidswell Ltd v Talksport Ltd[7] a Formula 1 driver was photographed holding a mobile telephone. The image was manipulated so that he looked as though he was listening to a portable radio, which had the words "Talk Radio" on it. The judge held that the photograph amounted to passing-off and acknowledged that celebrities have a property right in their image which is capable of protection. Similarly, the runner, David Bedford, succeeded in a complaint to Ofcom about an advertisement for a directory enquiry service which used "look alikes". He complained of breach of the Advertising Standards Code r.6.3, which provides that living persons must not be portrayed, caricatured or referred to in advertisements without their permission. The advertisements, however, were not banned, despite the finding in David Bedford's favour.

There may be a clear distinction between those cases where the complainant has a commercial interest in protecting an image and those where the complainant is protecting personal privacy, such as JK Rowling's action to restrict the use of images of her children to protect their privacy[8]. In other cases the distinction may be less clear, as in the *Douglas* case where there was both a commercial and privacy interest in images. However the courts have provided remedies for misuse of photographic images in both cases. Images may also be protected where there is neither a commercial interest or a specific privacy interest (see later in relation to the taking and use of photographs).

PROTECTION OF REPUTATION

2–04 The right to the protection of reputation is a right which falls within art.8 as an element of private life (*Re Guardian News & Media Ltd*[9]). The relationship between this aspect of the right and actions for defamation has arisen in a number of cases. In *Jane Clift v Slough BC*[10] Ms Clift brought an action for libel against the Council arising out of the publication of Ms Clift's name on the Council's Violent Persons Register. The Council accepted that the description of her as a person "who posed a medium risk of violence" was defamatory; however, it

[6] [2005] EWCA Civ 595, CA; [2007] UKHL 21.
[7] [2002] EWHC 367.
[8] The case law on photographs and privacy is dealt with below.
[9] [2001] UKSC 1.
[10] [2010] EWCA Civ 1171.

defended the publication which was made to a surprisingly wide range of staff and partner bodies on the basis of qualified privilege. It asserted that there was a duty on the Council to protect the safety of its staff and the staff of connected organisations and those persons who received the copy of the Register had an interest in receiving the information.

One of the issues at stake was the very widespread dissemination of the Register. On behalf of Ms Clift it was argued that qualified privilege can only apply where the party publishing has a duty to publish material to those who have a corresponding interest or duty in receiving it. For a public authority this must be consistent with its duties under public law and such duties must be carried out in accordance with the HRA. Therefore if art.8 is engaged by a publication the authority must be able to justify the publication under art.8 and meet the tests of legitimacy, justification and proportionality. The position was accepted by the Court which held that the wide publication failed to meet the test of proportionality:

> "Ill considered and indiscriminate disclosure is bound to be disproportionate".[11]

The wide publication breached Ms Clift's art.8 rights and was unlawful. Any argument for a duty to publish fell away and with it the possibility of a defence of qualified privilege.

As an alternative, the Council sought to argue that Ms Clift should have brought an action under art.8 rather than an action in libel. The Court did not accept this and made clear that the complainant was entitled to choose her cause of action.

2–05 The relationship between defamation and an action for misuse of private information, however, may be rather more difficult to navigate where a claim is made for injunctive relief and the facts complained of are discreditable but true. It is a complete defence to an action in defamation that the information complained of is true; a court cannot give the complainant any remedy in defamation if the facts complained of are true irrespective of whether there is a public interest in the publication. In addition, the rule in *Bonnard v Perryman*[12] precludes the grant of an injunction to restrain the publication of defamatory material before trial where defendant will claim justification:

> "We entirely approve of, and desire to adopt as our own, the language of Lord Esher, M.R., in Coulson v. Coulson– 'To justify the Court in granting an interim injunction it must come to a decision upon the question of libel or no libel, before the jury have decided whether it was a libel or not. Therefore the jurisdiction was of a delicate nature. It ought only to be exercised in the clearest cases, where any jury would say that the matter complained of was libellous, and where, if the jury did not so find, the Court would set aside the verdict as unreasonable'[13]."

However, in privacy cases publication can be restrained even where the information is true. In addition the threshold for the grant of injunctive relief to restrain publication is not the same. Where an application is made for an

[11] [2010] EWCA Civ 1171 per Ward L.J. at para.35.
[12] [1891] 2 Ch. 269.
[13] Per Lord Coleridge C.J.

injunction to restrain publication on privacy grounds pending trial, the test is that the applicant is more likely than not to succeed at trial.[14] In *RST v UVW*[15] an individual applied for an injunction to prevent the publication of information that he had previously paid a lady to provide sexual encounters which took place at his home and had entered into a confidentiality agreement with her under which he had provided consideration for her silence. The claim was advanced in privacy rather than defamation. The courts considered the point that a claimant is entitled to choose his cause of action where more than one is available to him[16]but noted that there is dicta in which it is suggested that, in cases in which it may be an abuse of process, a claimant should not be able to obtain an injunction in privacy where the court takes the view that the real issue is protection of reputation.[17] In that case the interim injunction was granted given the circumstances of the case. However in *LNS v Persons Unknown*[18] the footballer, John Terry, failed in an application for an injunction to prevent publication of the fact that he had had an affair and related personal information.

Mr Terry was married and held a number of apparently lucrative sponsorship deals. Giving judgment, Tugendhat J. noted that there could be an overlap with defamation in a limited number of privacy cases and suggested four broad groups of privacy cases being:

- those where the information complained of cannot be said to be defamatory, such as *Murray* where the law of defamation is irrelevant;
- those where, although the law of defamation overlaps with the privacy claim, the protection of reputation is not in fact the nub of the claim;
- those where the law of defamation overlaps with the privacy claim but the claim relates to conduct which would be unlawful and voluntary, for example financial irregularities, and where it would be unlikely that there would be any inconsistency in the treatment of the cases in relation to injunctions as the remedy would not be available under either head; and
- a limited group of cases where the conduct in question is not unlawful although it involves conduct which is voluntary and discreditable in some way (and by implication the claimant may be protecting reputation as well as privacy or that the protection of reputation may be in reality the nub of the claim).

The judge did not go on to set out in which types of cases claimants would be more likely to succeed, though it is implicit that applications for interim injunctions would be more likely to succeed in the first two types of cases than in the others. He also noted that it was for the applicant to determine which form of action he chooses to bring. However it is implicit that, if an applicant chooses to bring an action for misuse of private information in a case in which he really seeks to protect reputation, the court can weight that in deciding whether to grant injunctive relief. In this particular case the judge declined to make any of the orders sought, which included an injunction against any person who threatened to

[14] *Cream Holdings Ltd v Banerjee* [2004] UKHL 44.
[15] [2009] EWHC 2448 (QB).
[16] *Joyce v Sengupta* [1993] 1 W.L.R. 337.
[17] *McKennit v Ash* [2006] EWCA Civ 1714.
[18] [2010] EWHC 119 (QB).

publish the fact of Mr Terry's extra-marital relationship or any details of it. One of the reasons for the refusal was that it was likely that the "nub of the applicant's complaint is to protect [LNS's] reputation in particular with sponsors, and so (a) the rule in *Bonnard v Perryman* precludes the grant of an injunction; and (b) in any event damages would be an adequate remedy for LNS".

BACKGROUND–PRIVACY RIGHTS

2–06

As has been explained in Ch.1, the immediate predecessors of Directive 95/46/EC were Treaty 108 and the OECD Guidelines, although those instruments themselves owed their existence to the acknowledgement of the right to respect for private and family life in art.8 of the Convention. Directive 95/46/EC refers directly to art.8. Article I of Directive 95/46/EC states that one of the objects of the Directive is the protection of

> "...the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

While those interpreting the 1984 Data Protection Act tended to look back primarily to its immediate predecessors, particularly Treaty 108,[19] since the 1998 Act came into effect the courts have looked to the Directive and sometimes art.8 directly[20]. At EU level, the importance of informational privacy has been emphasised by the inclusion of data protection in the Charter of Fundamental rights of the European Union. Article 8 specifically covers personal data protection:

> "1. Every person has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority." [21]

Even before the Charter entered into force the Court of First Instance commented:

> "although [the Charter] does not have legally binding force, it does show the importance of the rights it sets out in the Community legal order".[22]

In the UK the implementation of the Convention rights in the Human Rights Act has brought an increased familiarity and ease with the application of the right to

[19] See the judgments of the Data Protection Tribunal (as it was then) in the cases of *Equifax Europe Ltd v Data Protection Registrar* Unreported June 28, 1991.
[20] See *Brian Robertson Reid v Secretary of State for the Home Department* (284/2011).
[21] See Ch.1 para.1-43 for a discussion of the Charter.
[22] *Philip Morris International and others v Commission* [2003] ECR II-I para.122 cited in the Opinion of the Advocate General in the PNR cases C-317/04 and C-318/04 at para.23.

respect for private life which is increasingly reflected in the case law. That case law has gradually moved the UK towards the development of a privacy right which would have been unthinkable only a few years ago.

UK background

2–07 The Younger Committee discussed the idea of privacy in its report[23] in 1972 and reviewed the various efforts over the years to define it.

David Calcutt, Q.C. in the *Report of the Committee on Privacy and Related Matters* in 1990,[24] after rehearsing the difficulties in coming to a satisfactory definition, posited a working one as:

> "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information",

and concluded that:

> "a natural person's privacy shall be taken to include matters appertaining to his health, personal communications and family, personal relationships and a right to be free from harassment or molestation."

Other analyses echo the themes of the right to choose to be alone or seek companions of one's choice, to control the information publicly known about oneself, to seek seclusion and to be free from outside interference in one's own domain.[25] In the context of the Convention, it is part of a package of rights which overlap and intersect, but all of which support the same core values to assert and protect the autonomy and dignity of each human-being.

CONFIDENTIALITY—BEFORE OCTOBER 2000

2–08 The Younger Committee did not consider that a general protection should be afforded to private life but recommended some new remedies to deal with areas of specific mischief. It also commented on the development of the law of confidence, which it thought provided a basis for developing privacy protection. It recommended that the Law Commission should reconsider the action for breach of confidence with a view to such further development.[26] The Law Commission duly reported in 1981 and recommended codification of the law of confidence. The report was never acted on and in 1998, in answer to a Parliamentary question,[27] the Lord Chancellor, Lord Irvinge of Lairg, stated that the report, Breach of Confidence (Law Commission Report No.110), would not be implemented given that the development of the case law had clarified the scope and extent of the breach of confidence action since its publication.

[23] The Younger Committee Report, Cmnd.5012 July 1972.
[24] Cmnd.5012.
[25] See Westin and others.
[26] See Toulson and Phipps, *Breach of Confidence* (Sweet and Maxwell, 1996), p.112, para.9.01.
[27] (*Hansard*, March 19, WA 213) Jul 29, 1998: col.WA202.

In the next section we trace that development of the tort of misuse of private information from the law of confidence however it should be recognised that the case law has not developed a general law of privacy. The cases examined in this chapter examine only the area of informational privacy. Other areas of law are related to privacy protection, trespass, nuisance, action for harassment, or defamation, but we are still a long way from a general privacy right.

The tort of misuse of private information has been developed from the law of confidence. In *A v B & C*,[28] which is described below, Lord Woolf L.C.J. said that, in cases on art.8, citation of authorities which relate to the action for breach of confidence prior to the coming into force of the 1998 Act "are largely of historic interest only". Nevertheless, anyone advising in this area will find it helpful to understand the evolution of the current cases.[29]

Development of jurisprudence on confidentiality

2–09 The case usually cited as the first major case in the area of personal confidentiality is *Prince Albert v Strange*.[30] When the facts are considered it seems but a short distance to *A v B & C* and surprising that it took 153 years to make the journey (*A v B & C* was decided by the Court of Appeal in March 2002). In the former case, Prince Albert had made some private etchings which he wished to have copied. He placed them with a printer in Windsor to have copies made. An enterprising employee took extra copies which were then offered for sale to the public via a sale catalogue in which they were described, not pictured, and which gave the impression that they were being published with consent. The Prince took Mr Strange, the publisher of the catalogue, to court to stop publication and succeeded.[31] The Prince had no pre-existing relationship with Mr Strange. There was no contract between them. The Court held that there was an infringement of the Prince's rights in the material and that there had been some breach of trust. It was suggested in the judgment that the breach of trust or confidence in itself entitled the Prince to a remedy.

The textbooks report relatively few cases in the same area over the next 100 years. The courts seem to have been little troubled by cases claiming breach of confidence in personal matters, although there seems to have been a gradual recognition of confidentiality in those relationships where sensitive information most commonly passed between two people.[32] The relationships of bankers, doctors, lawyers, clergy or other counsellors as well as other professionals with their clients are all regarded as confidential.

2–10 An extra-judicial development worthy of mention is the article published in the *Harvard Law Review* in 1890 in which the authors, Samuel Warren and Louis B. Brandeis, argued vigorously for a law of privacy to restrain the intrusions of the press. It has been much cited since.[33]

[28] [2001] CA 2086.
[29] For the material in the following section I am much indebted to Toulson and Phipps, above, and Francis Gurry, *Breach of Confidence* (Clarendon Press, 1984).
[30] (1849) 1 Mac. & G. 25.
[31] For a discussion of the historical basis of the action and this case in particular, see Toulson and Phipps.
[32] Gurry, above at p.143 onwards.
[33] 4 *Harvard Law Review* 1890.

The next significant case was *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd*.[34] Although this did not concern personal relationships, it confirmed two features of the action for breach of confidence which were essential for its future vigorous development: there did not have to be a contractual relationship between the parties before breach of confidence could be claimed and, where there was no contract, the action could be used to protect a wide range of subject-matter as long as it was not "public property or public knowledge". The generous approach taken to both the relationships and subject-matter capable of being protected meant that confidentiality could be invoked in a range of situations.

2–11 As the action for breach of confidence developed over the next 20 years, most of the reported cases concerned commercial or employment cases. However, in *Argyll v Argyll*[35] the Duchess of Argyll was successful in stopping her husband from disclosing information about the marital relationship. In that case the court confirmed that the doctrine could be applied in personal matters; rejected the argument that confidentiality could only be argued in a limited class of (primarily commercial) cases; and reiterated that this was a broad jurisdiction.

In 1981, the Law Commission produced a *Report on Breach of Confidence*.[36] The report reviewed the development of the law in this area. The review was no easy task. The body of case law on breach of confidence had grown organically. It had taken and used ideas from other areas. It had provided remedies where it thought they were needed. It had been messy, patchy, haphazard, vigorous and unplanned. There was no agreement on the legal basis of the right (a property right, contract, equity)[37]; the nature of the exemptions (are they exceptions to the obligation or defences to a breach?)[38]; the availability of damages (are they available or can only an injunction be issued?)[39]; or the effect on third parties (in what circumstances could they be bound if they came into possession of the confidential material?).[40] Not surprisingly the Law Commission proposed that these uncertainties and anomalies should be tidied up and the action for breach of confidence put on to a statutory footing. The report was never acted upon. If it had been, the privacy jurisprudence of the last decade might not have been possible.

The publication of personal information which has been unfairly obtained was considered in a number of cases over the following years. In *Stephens v Avery*[41] the defendant had betrayed her friendship with the plaintiff by providing a newspaper with details of the plaintiff's sexual life. The plaintiff claimed damages for breach of confidence. In *Francome v Mirror Group Newspapers*[42] a home telephone was bugged and the conversations over it taped by strangers. The resulting information was sent to the newspaper. In restraining publication before the trial, the Court of Appeal recognised that the conversations were confidential.

[34] (1948) 65 R.P.C. 203.
[35] [1967] Ch. 302.
[36] Cmnd.8388 (1981).
[37] Gurry, above, Ch.2.
[38] Gurry, Chs 15 and 16.
[39] Gurry, Ch.23.
[40] Gurry, Ch.13.
[41] [1988] 1 Ch. 419.
[42] [1984] 1 W.L.R. 892.

On the other hand, some judges were reluctant to protect information about those whose lives were in the public domain. Plaintiffs failed in *Woodward v Hutchins*[43] and *Lennon v News Group Newspapers Ltd*.[44] In the first case, the *Daily Mirror* wanted to publish material about a number of pop stars and the court refused to restrain the publication as it said that they had already put their lives in the public domain. In the second, the *News of the World* wanted to publish material about John Lennon's first marriage. The Court of Appeal said that the relationship had ceased to be private and refused to stop publication. The two cases have been distinguished in latter cases and can no longer be regarded as sound authority.

In *Attorney-General v Guardian Newspapers Ltd (No.2)*,[45] the *Spycatcher* case, the judges expressed a range of views on the action for breach of confidence and its application to personal information which have been much cited in later cases. A former member of the security services had published a book of memoirs of his time with the service. The government tried to restrain publication of material from the book in the *Guardian* newspaper, even though it had been published outside the United Kingdom and the UK Government had been unable to restrict its publication abroad. The Government claimed that the disclosure of information by the individual was a breach of confidence. Lord Goff, in his judgment, described the position that the law of confidence had reached at the end of the last century, although he disclaimed any intention to produce a definitive description of the area (ineffectually, as every text book cites it).

Lord Goff said that a duty of confidence arises when:

> "confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others".

2–12 There can be no confidentiality unless the information is "confidential", that is it has not entered the public domain; the duty does not apply to information which is trivial or useless and confidentiality can, in some circumstances, be negated by public interest.

In the same case, Lord Keith signalled a green light for future privacy cases by accepting that privacy was a right capable of protection by the law of confidence.[46]

It might have been thought that after such encouraging dicta the courts would have moved forward to develop the action for breach of confidence into one which offered a more general protection for personal privacy. However, the decision in *Kaye v Robertson*[47] the following year proved a setback and, although the decision was later criticised, over the decade before the Human Rights Act came into force even the keenest proponents of judicial activism in this area faced difficulties in seeking to develop a more general right of privacy because of the chilling effect of the decision. In this case the subject had been in an accident,

[43] [1977] 1 W.L.R. 760.
[44] [1978] F.S.R. 573.
[45] [1990] 1 A.C. 109.
[46] [1990] 1 A.C. 109 at 255.
[47] [1991] F.S.R. 62.

which had resulted in severe injuries. A journalist entered his hospital room without permission and photographed him. The photograph was published. The action was taken against the photographer. Although the entry was wrongful, being a trespass, and the Court of Appeal acknowledged that the publication was an appalling invasion of his privacy, it refused to grant an injunction restraining publication. As a number of commentators have subsequently pointed out, the Court was not referred to the developing cases on confidentiality, presumably because the intrusion was by a stranger. It must also be borne in mind that the case was decided at a time when possible legislation restricting freedom of the press was a live issue.[48] The Court, recognising that a decision to protect the actor's privacy would be going beyond the boundaries of the law of confidence and, presumably, the wider political context, reaffirmed that the UK law knew no right of privacy and that it was a matter for Parliament, not the courts, to develop one. If the Court hoped that this principled abstention from developing the law would stir Parliament into action over press excesses it was to be disappointed. However, the clarity of the judgment was to prove a setback for those who advocated the development of a judge-made right to personal privacy for nearly a decade. In *R. v Khan*,[49] a case which was later considered by the ECtHR,[50] the House of Lords reiterated that in the United Kingdom there was nothing unlawful about a breach of privacy.

Development continued in related areas, and in *Hellewell v Chief Constable of Derby*[51] the court considered the disclosure of personal information which had been obtained under compulsion by a public body. This was partly a response to a wider development of information sharing by the public sector with increased privatisation, moves to partnership workings with the private sector and the disclosure of information between government departments and other public bodies, for example via data matching initiatives. Concern had previously been expressed at such developments and the limitations on the powers of public bodies to use and disclose personal information was emphasised in *Marcel v Commissioner of Police for the Metropolis*[52] by the Vice Chancellor who had memorably commented that: "... the dossier of personal information is the hallmark of the totalitarian state".

2–13 In a number of cases the courts held that personal information obtained under compulsion would be subject to an obligation of confidence in the hands of the public body.[53] In *Hellewell* the local police force had provided shopkeepers with photographs of a known shoplifter. The photographs had been taken under compulsion when the individual was in custody. The individual complained of breach of confidence. It was held that there was an obligation of confidence owed to the individual as the information had been extracted under compulsory powers and the police were limited in the uses they could make of the information. In the particular case the disclosure of the photograph was justified in the public interest. More importantly for the purposes of the development of a more general

[48] See discussion in Ch.17 on the exemption for journalism.
[49] *The Times*, May 5, 1996.
[50] ECtHR report, *The Times*, May 23, 2000.
[51] [1995] 1W.L.R. 804.
[52] [1991] All E.R. 845; [1992] 1 All E.R. 72, CA.
[53] *Alfred Crompton Amusement Machines v Commissioner for Customs and Excise (No.2)* [1973] 2 All E.R. 1169.

privacy right, the judge commented that the law of confidence would be able to protect someone from an invasion of privacy caused by being photographed without consent from a distance.

The comment was obiter and was not followed in *R. v Brentwood BC Ex p. Peck*.[54] In that case the court dismissed a claim that the local council had acted unlawfully in giving the media copies of a CCTV recording of Mr Peck engaged in a suicide bid in a public place. It should be noted, however, that Mr Peck was later successful in his action against the UK in the ECtHR at Strasbourg . He succeeded not only on art.8 but also art.13 as the Court held that he had no effective legal remedy in the UK in relation to the violation of his right to respect for private life.

In *R. v Chief Constable of the North Wales Police Ex p. Thorpe*,[55] the disclosure of information about an individual's previous criminal history of offences against children by a public authority was considered by the court and held to be justified in the circumstances.

Thus, despite the uneven growth of authority in this area, by the time the HRA came into effect the law of confidence had developed significantly in the United Kingdom and there were persuasive dicta that an action for breach of confidence might be employed to protect personal privacy.

The action for breach of confidence offers a useful starting point for the development of a privacy right. There is no absolute right to confidentiality. Confidentiality may be breached where an opposing interest outweighs the obligation. Thus confidentiality will give way to an order of the court, legal compulsion, or a greater public interest in the disclosure. As such it incorporates a balancing test that makes it a malleable tool to apply where balances have to be struck, particularly between art.8 and other rights.

2–14 The European Court recognised the development of the law of confidence in the United Kingdom and its growing potential to protect personal privacy in *Wiener v United Kingdom*[56] and *Earl and Countess Spencer v United Kingdom*.[57] In both cases the applicants chose to bring cases in Strasbourg on the grounds that the United Kingdom did not offer the remedies they needed to protect their privacy rather than try to bring actions in the UK courts. In the *Wiener* case various statements had been made about the plaintiff's relations with his wife, not all of which were true. The court held that the UK law afforded sufficient remedies to protect his reputation (including libel, in respect of which he already had obtained a settlement), but said the failure to take action for breach of confidence did not amount to a failure to exhaust his remedies in the United Kingdom due to the uncertainty and lack of clarity in the jurisdiction. In the *Spencer* case, the Earl and his wife had been subject to articles in the newspapers about their marriage and about her health problems and photographs taken without consent. To that extent it was not dissimilar to the situation in which Naomi Campbell later found herself. The Commission declared the complaint to the court inadmissible as the applicants had not exhausted their domestic

[54] [1998] E.M.L.R. 697; *The Times*, December 18, 1997, QBD.
[55] [1999] Q.B. 396.
[56] Application 1087/84; (1986) 48 DR154, EComHR.
[57] Application 28851/95; (1998) 36 E.H.R.R. CD105.

CHAPTER 9

Notification

INTRODUCTION

Transparency, or openness about the uses of personal data, is a key element in data protection; this is reflected in the right of subject access and the importance of the fair processing notice rules. The public register of data controllers contributes to the transparency of data processing. The system of notification also provides funding for the Office of the Information Commissioner. Until October 2009 this was achieved by way of a flat fee however since that data a two tier arrangement has been introduced and larger data controllers now pay a fee of £500. Notification does not have a regulatory aspect, unlike registration under the 1984 Act. Registration under the 1984 Act could be refused where the Registrar believed that the applicant would not comply with the principles. Under the 1998 Act the Commissioner cannot refuse to place any entry in the register, as long as the application is properly made. **9–01**

The details of the notification scheme do not appear in the primary legislation. The 1998 Act sets out only the outline provisions. The detail is to be found in a number of statutory instruments and administrative arrangements made by the Commissioner. The relevant SIs are the Data Protection (Notification and Notification Fees) Regulations 2000, the Data Protection (Notification and Notification Fees) (Amendment) Regulations 2001 and the Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009.[1] The administrative arrangements are set out in the *Notification Handbook: A Complete Guide to Notification*.[2] The Regulations include some central aspects of the system, for example some of the exemptions from the obligation to register.

SUMMARY OF MAIN POINTS **9–02**

(a) Notification is not a control mechanism; the Commissioner cannot refuse a notification and exemption from notification confers no exemption from other aspects of the Act.

(b) The information to be notified covers the data, the purposes of processing, data subjects, recipients, and overseas transfers but does not include sources of the data.

[1] SI 2000/188, SI 2001/3214 and SI 2009/1677.

[2] July 2010 edn, available from the ICO website.

(c) An entry on the register lasts for one year and must be renewed annually. An annual fee applies which is set as £35 for data controllers in tier one and £500 for data controllers in tier two. The tier is determined by the number of staff and turnover.

(d) Security information must be notified to the Commissioner but does not appear on the public register.

(e) There is a provision for some processing to be designated "assessable processing". Such processing must be notified to the Commissioner before the commencement of the processing for the Commissioner to assess. No categories of processing have been designated as assessable processing to date.

(f) Manual data does not have to be notified unless it falls into an assessable processing category.

(g) There are a number of exemptions from the obligation to register, some of which are set out in the Act itself and others of which are set out in the regulations.

(h) Those who are exempt from making an entry on the public register must still be able to provide an inquirer with information equivalent to that contained in the register; alternatively, voluntary notification is allowed if the data controller wants to make a public statement of processing available.

(i) Only one register entry per data controller is permitted and purpose titles may usually only be used once.

(j) Public authorities must state their status on the register following an amendment introduced by the Freedom of Information Act 2000.

(k) Data processors are not required to notify, unlike computer bureau which were required to register under the 1984 Act.

THE DUTY TO NOTIFY

9–03 Section 17(1) provides that personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Commissioner. Under s.21(1) the data controller is guilty of an offence if such processing takes place.

Scope of duty

9–04 The duty is imposed on all data controllers unless an exemption can be claimed. Controllers do not have to notify if:

(a) the personal data are exempt from Pt III of the Act. This applies to data held for personal, domestic and recreational purposes under s.36 or if the purposes of national security require that the personal data should not be registered (i.e. should not be put into the public domain).[3] Personal data which are exempt from Pt III are also exempt from prior assessment;

[3] s.28.

(b) the sole purpose of the processing is the maintenance of a public register under s.17(4). In theory such processing may still be subject to prior assessment but in fact this would be most unlikely;

(c) the data are manual data covered by the Act. This exemption is provided by s.17(2). Such data may still be subject to prior assessment; or

(d) the data fall under one of the exemptions to the duty to notify in the notification regulations.

A data controller is entitled to choose the purposes for which he is registered and as long as those are lawful purposes the Commissioner cannot interfere with his choice or restrict the nature of the purpose.[4]

Processing exempt from notification

Exemptions under the Act

These cover: 9–05

(i) any personal data if the exemption is required for the purpose of national security (s.28 (1));

(ii) personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (s.36);

(iii) processing whose sole purpose is the maintenance of a public register (s.17 (4)). "Public register" is defined in s.70 as any register which is open to public inspection or open to inspection by any person having a legitimate interest either by or under an enactment or in pursuance of any international agreement;

(iv) Manual data which fall within the definition of a "relevant filing system".

The exemptions will be narrowly construed. In the case of *Bodil Linqvist v Alklagarkammaren I Jonkoping*[5] the European Court considered the relevant provision in the Directive and held that posting information about members of a congregation on a website would not be covered by the exemption for personal or domestic processing.[6] In the Notification Handbook the point is made in respect of the exemption for public registers that the exemption only applies to the information held on the register and not ant information required to compile it.

Other exemptions

Further exemptions may be prescribed by the Secretary of State but only in cases where it appears to him that the processing is unlikely to prejudice the rights and freedoms of data subjects. In order to comply with art.18(2) of the Directive which sets out the circumstances in which exemptions from notification may be permitted the Secretary of State must specify: 9–06

[4] *Chief Constables of Humberside v Information Commissioner* [2009] EWCA Civ 1079.

[5] [2003] E.C.R I-1297.

[6] See Ch.3 for a full discussion of the *Linqvist* case.

(i) the purposes of the processing;
(ii) the data or categories of data undergoing processing;
(iii) the category or categories of data subject;
(iv) the recipients or categories of recipients to whom the data are to be disclosed; and
(v) the length of time the data are to be stored.

9–07 Five exemptions from notification are contained in notification regulations. A data controller must comply with the remainder of the Act even if he is exempt from notification. Moreover, if requested he must be able to produce a description of his processing in accordance with s.24. The exemptions will not apply if the processing is assessable processing,[7] although no categories of assessable processing have been declared.

The categories of exempt processing set out in SI 2000/188 are:

- processing for staff administration;
- processing for advertising marketing and public relations;
- processing for accounts and record keeping; and
- membership processing of membership information by non-profit making bodies.

The first three together are sometimes referred to as the "core business purposes" and mean that a small business may be exempt from the requirement to notify as long as the processing remains strictly within those limits. In each case the nature of the processing, the data held and the range of acceptable disclosures are described in the Regulations and the data controller must stay within those bounds to be able to claim the exemption. In each case the exemption is not lost where disclosures are made under the non-disclosure exemptions or where they are required by any enactment, rule of law or order of the court.[8]

For each exemption the purpose of the processing, the types of personal data, the types of data subject, the nature of the permitted disclosures and the length of time for which the data are to be held are set out. If the data controller processes outside these parameters he will lose the benefit of the exemption. However, where the data are required for research and fall within the research exemptions it would presumably be possible for the data controller to continue to hold the data for research purposes within the terms of that exemptions. In such a case a notification covering the research purpose would be required. In addition disclosures may be made under the non-disclosure exemptions. This means that in each case the data may also be disclosed where the particular conditions are fulfilled in the following cases:

- where there are statutory requirements or court orders;
- for the purposes of national security;
- for the purposes of the prevention or apprehension of offenders, prevention or detection of crime, assessment or collection of any tax or duty;
- for journalistic, literary or artistic purposes;

[7] SI 2000/188 reg.3.
[8] SI 2000/188 reg.3(b).

- for the purpose of or in connection with any legal proceedings or for the purpose of obtaining legal advice or establishing legal rights; and
- where the data controller is obliged to make the data public.

Staff administration

9–08 This is described as processing for the purpose of:

> "appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller".[9]

The data subjects may be past, present or prospective members of staff. Staff includes employees, office holders, workers under a contract for services and volunteers.[10]

The exemption therefore extends to not-for-profit organisations, such as charity shops, which use volunteers. Information may also be held on other data subjects where it is necessary for the data controller to process personal data about them for the exempt purpose. Thus data about the nearest relations of employees might be held for contact purposes or in connection with pensions.

The exemption only applies to data held about the staff of the data controller. So an organisation which handles pensions matters on behalf of a data controller could not rely on the exemption.

The personal data which may be held are limited to name, address, identifiers and information as to qualifications, work experience and pay or "other matters the processing of which is necessary for the exempt purposes".[11] Potentially this covers a wide range of information. Information about health matters, criminal convictions, trade union membership and other sensitive data are often held in relation to personnel and superannuation matters. The disclosure limitation is that the data may only be disclosed to third parties either where it is necessary to make the disclosure in order to carry out the exempt purpose or where the disclosure is made with the consent of the data subject.

The data must not be kept beyond the ending of the relationship between the data subject and the controller unless and for so long as is necessary for the exempt purpose.

Advertising, marketing and public relations

9–09 This is described as processing for the purpose of:

> "advertising or marketing the data controller's business, activity, goods or services and promoting public relations in connection with that business or activity, or those goods or services".

The data subjects may be past, existing or prospective customers or suppliers or any other person in respect of whom it is necessary to process personal data for

[9] Sch.1 para.2(a).
[10] Sch.1 para.1: "workers" has the meaning given in the Trade Union and Labour relations (consolidation) Act 1992.
[11] SI 2000/188 Sch.1 para.2(c)(iii).

the exempt purpose. This would allow, for example, the processing of personal data about contacts for the purposes of public relations. It is not apparent on the face of it why suppliers have been included as data subjects. Organisations do not usually market to their suppliers as such (unless they hope to convert them to customers) but if the intention is to cover such eventualities they would be covered as prospective customers. The term "prospective" is a wide one; however, it is difficult to see how a narrower term could have been used. The point in made in the *Notification Handbook* that a data controller can buy or rent a third party list for marketing purposes without losing the benefit of the exemption but if the controllers sells or rents his own contact or customer list he will lose it.

The personal data are limited to name, address and other identifiers or information which it is necessary to process for the exempt purposes. The purpose description is therefore the main restricting factor on the processing which may be carried out under the exemption.

Disclosures are limited to those where the disclosure is necessary for the exempt purposes or is made with the consent of the data subject but includes savings for disclosures made under enactments and the non-disclosure exemptions (see above).

The limitations on retention of data are the same as for staff administration as described above.

Accounts and records

9–10 This is described as processing for the purpose of:

> "keeping accounts relating to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by or to the data controller in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of such business or activity".

The data subjects may be past, existing or prospective customers or suppliers or any other person the processing of whose data is necessary for the exempt purposes. As noted above the term "prospective" is a wide term.

The data may consist of names, addresses and other identifiers together with information as to financial standing or other data which it is necessary to process for the exempt purposes.

Remote credit checks

9–11 The regulation provides that information relating to the financial standing of customers, suppliers or others does not include personal data processed by or obtained from a credit reference agency. This means that a data controller who carries out remote credit checks from a credit reference agency will not be able to claim the exemption even if he contributes no information and never downloads or otherwise retains the data. The fact that in such cases he does not become a

data controller for the credit reference agency data was confirmed by the decision of the Court of Appeal in *Johnson v Medical Defence Union*.[12] In *Johnson* the member of staff employed by the MDU consulted the computer records of references to Mr Johnson and summarised the material on hard copy before entering it into the computer again. The Court of Appeal held that there was no "processing" involved in the activity of reading the material and summarising it. This would appear to be on all fours with the situation of one who consults a credit reference agency in this way. In previous Guidance the Commissioner argued that the user of the credit reference agency services did become a controller but in the current edition the Handbook simply states that:

> "[This exemption] includes processing relating to deciding whether or not to do business with a particular customer or supplier but specifically excludes personal data processed by or obtained from a credit reference agency".

The rules relating to disclosures under the accounts exemption are the same as for the other exempt categories; that is disclosures can be made where necessary for the exempt purpose, with the consent of the data subject or under the non-disclosure exemptions.

The data must not be retained after the end of the relationship or so long as is necessary for the exempt purpose.

Processing by non-profit making organisations

This is described as processing carried out by a body or association which is not established or conducted for profit and is 9–12

> "for the purposes of establishing or maintaining membership of or support for the body or association or providing or administering activities for individuals who are either members of the body or association or have regular contact with it".

The data subjects may include not only the usual categories of past, existing or prospective members and persons in respect of whom it is necessary to process personal data for the exempt purpose but also any person who has regular contact with the body in connection with the exempt purposes. Accordingly, charities are able to keep records of regular beneficiaries without losing the exemption. Interestingly, this appears to mean that the body will lose the benefit of the exemption if it retains records of those contacts who only donate or assist on a "one off" basis.

The personal data may consist of names, addresses and identifiers, information as to eligibility for membership and data necessary for the exempt purposes.

As in the other exemptions disclosures are limited to those made with consent, those necessary for the purpose or those made under the non-disclosure provisions.

The data must not be retained beyond the ending of the relationship except so far as is necessary for the exempt purposes.

[12] [2007] 1 All E.R. 467.

Processing for judicial functions

9–13 A further exemption was added by SI 2009/1677 and came into effect on July 31, 2009.[13] The terms of this exemption are not in the same format as the others and it is not clear that they meet the requirements of art.18(2) of the Directive which specifies the level of detail required for an exemption from notification (see para.9–06 above). The category of data controllers and the purpose of the processing are specified but not the data or categories of data, the recipients or categories of recipients or the length of time that the data are to be stored for. It is possible that these may have been specified in some administrative form by the Court Service however we have not been able to trace any relevant documents at the time of writing.

9–14 The exemption applies to the processing by a judge or a person acting on the instructions or on behalf of a judge. A judge includes:

- a justice of the peace or a lay magistrate in Northern Ireland;
- a member of a tribunal; and
- a clerk or other officer entitled to exercise the jurisdiction of a court or tribunal.

A tribunal means any tribunal in which legal proceedings may be brought. The processing is exempt if it is,

> "for the purpose of exercising judicial functions including functions of appointment, discipline, administration or leadership of judges".

There is no further gloss to this description which appears to cover a wide scope.

THE REGISTER

Contents of the register

9–15 Section 16(1) sets out the particulars which the data controller must specify in the public register. The particulars set out in s.16(1) are:

- name and address of data controller;
- identity of a representative (if any);
- description of the personal data being processed and the categories of data subjects;
- description of the purposes of the data processing;
- description of the recipient or recipients of the data;
- names or description of the territories outside the EEA to which the data are to be transferred; and
- statement of exempt processing.

[13] SI 2009/1677 reg.2, amending SI 2000/188.

9–16 Section 71 of the Freeedom of Information Act 2000 added a provision which requires public authorities to also include a statement of the fact that they are public authorities for the purpose of the FOIA.

Name and address of data controller

9–17 Under s.16(3), the address given for a registered company must be that of its registered office. The address of any other person carrying on a business must be that of his principal place of business in the United Kingdom. The name should be the name by which the person is legally known: in the case of a registered company, its registered name rather than a trading name; in the case of an organisation other than a registered company, its full name as set out in its constitution or other formal document; and in the case of an individual, the name by which he is usually known.

Name and address of nominated representative

9–18 The previous registration system also included a non-statutory, contact name for use by the Registrar's office. A data user could choose to have correspondence about his entry sent to a nominated contact. This was a useful service for some data users. There is now a provision allowing a controller to include the name and address of a representative where he "has nominated a representative for the purposes of the Act". This is a new provision. It is not amplified in any other part of the Act. There is a requirement in s.5 that a person established overseas without a branch or agent in the jurisdiction who processes personal data in the United Kingdom other than merely for transit must nominate a representative. This appears to contemplate that a data controller may nominate a representative within the jurisdiction to deal with all or some of his data protection matters. Presumably the representative need not be an employee and might be a professional or specialist adviser who deals with data protection matters on behalf of clients. The inclusion of a named representative is not a substitute for the name of the data controller. It cannot be used as a method of avoiding the name appearing on the public register. It is to be included, if at all, as an additional piece of information.

Recipients

9–19 In the 1984 Act, both sources and disclosures of personal data had to be registered. Sources no longer figure on the register and disclosures have been replaced by recipients. These are persons to whom data are disclosed other than in pursuance of a legal obligation.

Form of notification

9–20 The Regulations provide that the form of giving notification shall be determined by the Commissioner. Thus the detail of the data subjects, data classes, purposes, recipients, overseas transfers and security measures are determined by the Commissioner. The Commissioner also determines how changes in notification

under the Act are to be presented. Information about the notification scheme is available in the *Notification Handbook* from the OIC website. The introduction makes clear that notification is not intended to be a detailed system:

> "It is not however intended and (nor is it practicable) that the register should contain very detailed information about a data controller's processing. The aim is to keep the content at a general level, with sufficient detail to give an overall picture of the processing. More detail is only necessary to satisfy specific statutory requirements or where there is particular sensitivity".

The system remains purpose led, as it was under the 1984 Act. The system is template based. When notifying online, the controller selects the business type which most nearly matches his business from a list and an application template comes up which includes those purposes most commonly used by businesses of that type together with the data classes, subjects and recipients most commonly used in connection with each purpose. The controller can amend the template by adding or removing purposes or adding or removing other categories of information. Telephone applications follow the same pattern. If the application is made on an application form the controller may chose purposes and other categories from the standard lists. There are a number of standard purposes, data subject classes, data classes and recipients. If none of the standard purposes fit the applicant should describe the purpose in his own words.

As will be appreciated from the standardised nature of the system the descriptions are presented in broad terms. The controller must specify the final destination of personal data if they are to be transferred indirectly through an EU state. The description of overseas transfers is the broadest of all. The applicant has a choice of registering either:

- none outside the EEA;
- worldwide; or
- naming up to 10 individual countries.

Statement of exempt processing

9–21 Where applicable, a notification must contain a statement that the controller also processes or intends to process personal data covered by a notification exemption or personal data which are part of a relevant filing system s.16(1)(g). This reflects the fact that not all personal data have to be included on the public register. Section 17(2) exempts from notification manual data which are otherwise covered by the Act, that is data held as part of a relevant filing system or manual data otherwise held as part of an accessible record. Further exemptions are made in the notification regulations. A data controller may choose to include any of these categories of exempt data in his register entry on a voluntary basis (see section on voluntary notification below) but if he is registered and decides not to include them his entry must state that he has not done so. The statement of exempt processing on the register is:

> "This data controller also processes personal data which are exempt from notification".

Additional information in the Register

Under s.19(2)(b) of the Act the Regulations may authorise or require the Commissioner to include other information in the register. Regulation 11 provides that the Commissioner may include: 9–22

- the registration number;
- the date the entry is treated as starting (which will be the date of receipt of the application);
- the date the entry expires; and
- contact information for the data controller.

These are all to be included. Data controllers are also asked to provide a company registration number, however this is not a requirement of the Regulations.

SPECIAL CASES

Under s.18(4), the Act allows special provisions to be made "in any case where two or more persons are the data controllers in respect of any personal data". Such provisions have been made in two cases, for schools and partnerships. 9–23

Schools

The Government was committed to dealing with the situation in which local authorities, governors of schools and head teachers all registered separately under the 1984 Act. This arose because the statutory provisions dealing with education impose separate legal obligations on the local education authority, the governors and the head teacher. Similar incidents of separate legal responsibility imposed on office holders occur in other areas of the public sector; for example, electoral registration officers were required to register separately from the local authority which employs them. It is not a universal pattern and some office holders on whom statutory duties are imposed registered under the name of the employing body. In many cases they were allowed to register under the name of the office, although the office did not have a legal personality of its own. These anomalies arose over the years, particularly as individual responsibilities were increasingly imposed on individual office holders by statute. Most of these have not been affected but special provision has been made for schools. Regulation 6 provides that in those cases where the head teacher and the school are both data controllers for the same data one notification may be given in the name of the school. 9–24

Partnerships

Although it is not expressly stated, the presumption appears to be that generally partners will be data controllers jointly or in common for data used by the partnership. The 1984 Act made no special provision for the registration of partnerships or indeed for any form of joint registration. This caused practical 9–25

problems for the Registrar's office. In the early years of the office, a pragmatic approach was adopted to allow partnerships to register under the partnership name, subject to providing the names of the current partners. However, the basis for this was not clear given that a partnership, in England and Wales at least, has no legal personality. It could give rise to problems where partnerships split up or where a small partnership was dissolved and one partner wished to carry on the business as a sole trader. In the former case, as long as the partnership name was retained, the Registrar's office allowed the registration to be maintained by the element of the former partnership which had retained the name; in the latter case the individual was required to re-register. Under the 1984 Act, the Registrar made administrative arrangements under which partners registered jointly for the personal data used in the partnership. Those arrangements were formalised and reg.5 provides that where persons carry on a business in partnership they may register jointly in the name of the partnership for personal data used for the purposes of the firm. The name and address to be specified is the firm's principal place of business. The names of the partners need not be supplied.

Groups of companies

9–26 No special provisions have been made for groups of companies. If companies in the same group are data controllers they must each notify separately. Trading names may be included in the register but not the names of other legal entities.

FEES

9–27 The Secretary of State is under an obligation, when setting fees, to have regard to the desirability of securing that the fees payable to the Information Commissioner are sufficient to offset the expenses of the Commissioner under s.26(2) and the expenses of the Secretary of State so far as attributable to the Commissioner's functions. The fees are no longer related to the cost of the Tribunal since it became part of the General Regulatory Chamber.[14] The fees are not retained by the Commissioner but nevertheless the amount brought in by the fees must be evaluated in the light of the costs of the Office. The fee for notification was previously set at £35 for all data controllers. This was changed by the Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009.[15] These changed the fee regime with effect from October 1, 2009. New notifications and renewals after that date have been subject to the new fees. The change is a response to the long-standing concern that the fee structure did not reflect the allocation of resource used by the Commissioner's Office. Large organisations in the public and private sector generally process far more information, and more sensitive information, than small and medium-sized enterprises. The tiered notification fee structure is intended to reflect the cost of the resource spent on regulating data controllers of different sizes. The House of Commons Justice Committee Report Protection of Private Data, published on January 3, 2008, noted that it was an anomaly that the same basic registration fee

[14] The Transfer of Tribunal Functions Order 2010 (SI 2010/22), amending s.26(2)(a).
[15] SI 2009/1677.

of £35 was paid by data controllers, irrespective of size. The Committee considered that a "graduated rate would be more appropriate, more likely to reflect actual costs, and more suited to providing an adequate income for the policing of data protection".

Between July 17 and August 27 2008, the Ministry of Justice ran a public consultation covering the fee change. It also held a stakeholder event on August 28 2008. The ICO reported that respondents to the consultation and attendees at the stakeholder event were overwhelmingly in favour of a tiered notification fee structure.[16]

9–28 There are two tiers of controller: tier one controllers who pay a fee of £35per annum, and tier two controllers who pay a fee of £500. A data controller is in tier two if it has been in existence for over one month and is either:

- a public authority with more than 250 members of staff; or
- is not a public authority, has a turnover of £25.9 million or more in the relevant financial year and 250 or more members of staff.

Public authorities are as defined in the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2003. Charities and small occupational pension schemes fall into tier one if they are required to notify, .i.e. are not exempt from notification. Notification regulations may prescribe the information about the data controller which is required for the purpose of verifying the fee payable for notification.[17] The power has not yet been exercised as the 2009 Regulations do not provide specifically for the provision of information to the Commissioner to verify the fees. The Regulations provide that where a data controller has been in existence for more than 12 months the "data controller's financial year" is defined as the most recent financial year ending before the notification fee is sent to the Commissioner in the case of a new notification or the date on which the entry expires in the case of a renewal.[18] The financial year in relation to a company is determined in accordance with s.390 of the Companies Act 2006 and for a limited liability partnership with that section as applied by the Limited Liability Partnerships (Accounts and Audit) (Application of Companies Act 2006) Regulations 2008.[19] If the data controller has been in operation for less than 12 months, the turnover is assessed on the basis of the period for which it has been in existence on the date that the fee is sent to the Commissioner. The term "turnover" is not defined in the Regulations but the document "Notification Fee Changes—What You Need to Know", which is available on the ICO website, states that turnover,

> "
> - in relation to a company, has the meaning given in section 474 of the Companies Act 2006;
> - in relation to a limited liability partnership, has the meaning given in section 474 of the Companies Act 2006 as applied by regulation 32 of the Limited Liability Partnerships (Accounts and Audit) (Application of Companies Act 2006) Regulations 2008; and

[16] "Notification Fee Changes—What You Need to Know 2009", available from the ICO website.
[17] ss.16(h) and 18(5A) added by Coroners and Justice Act 2009.
[18] reg.3 inserting new s.7A(3) into SI 2000/188.
[19] SI 2008/1911.

- in relation to any other case, means the amounts derived by the data controller from the provision of goods and services falling within the data controller's ordinary activities, after deduction of: trade discounts, value added tax, and any other taxes based on the amounts so derived."

It advises that groups of companies will need to assess the numbers of members of staff and turnover for each separate company in the group, not the overall group figures.

The SI sets out that numbers of staff are calculated by ascertaining the total numbers of people who have been members of staff of the data controller for each month of the relevant financial year, adding together the monthly totals and dividing by the number of months in the controller's financial year. The term "staff" will cover employees, office holders, and workers under a contract for service, partners and volunteers under the Schedule to SI 2000/188. Where information is provided to the Commissioner in order to enable him to verify the fee payable it will not appear on the public register.

9–29 There are specific provisions to deal with the special cases of registration for partnerships and schools (see above). In relation to a partnership registered jointly in the name of the partnership under reg.5 the turnover and members of staff are taken to be of the firm as a whole, which presumably includes the partners themselves. In relation to a notification in the name of a school under reg.6, the members of staff include the staff of the governing body and of the school. A charity in England and Wales has the meaning given by the Charities Act 2006 s.1; in Scotland means a body entered into the Scottish Charity Register maintained under s.3 of the Charity and Trustee Investment (Scotland) Act 2005; and in Northern Ireland has the meaning in s.1 of the Charities Act (Northern Ireland) 2008. Small occupational pension scheme is not defined in the Regulations but the ICO guide states that it has the meaning given in reg.4 of the Occupational and Personal Pension Schemes (Consultation by Employers and Miscellaneous Amendment) Regulations 2006.

9–30 No VAT is chargeable on the fee. Change to entries on the register of notifications is free. Over the last few years there have been a number of "scams" where organisations using similar sounding names to the OIC duped businesses into sending them money to register. A number have now been prevented from trading.

Fees cannot be returned once they have been paid except in exceptional circumstances. Any application for a refund should be made to the OIC setting out the grounds of the application.

GENERAL PROVISIONS

Number of entries permitted

9–31 The Commissioner must maintain a public register of those who give him notification of relevant data processing. He can only allow one entry in the register for each data controller, as under s.19(1)(b) he must make an entry following a notification from any person ". . . in respect of whom no entry as a data controller was for the time being included in the register".

Therefore, if a controller already has an entry in the register and purports to make a further application the Commissioner is under no obligation to accept it. Presumably the Commissioner will reject such a purported application as invalid. In the 1996 consultation paper, the Registrar recommended that each data user should only be able to make use of each standard purpose once and this has been put into effect, although the *Handbook* states that in exceptional circumstances the Office may allow the use of a purpose more than once "where we believe that it will aid transparency".

Refusal of a notification of entry

9–32 The Commissioner is given no specific power to refuse an application for notification as long as it is made in the prescribed form. The restriction of applications to the prescribed format should presumably ensure that he is able to treat a purported application for notification which is scurrilous, vexatious or incomprehensible as invalid on the ground that it is not presented in the prescribed form, but does not allow the refusal of any application in the prescribed form however unlikely its contents may be.

Duration of a register entry

9–33 An entry in the register lasts for 12 months or such other period as may be prescribed by the regulations, and different periods may be prescribed for different cases. The entry may be renewed on payment of the relevant annual fee. Fees may be paid by cheque, direct debit or BACS. If an entry is not renewed within the 12-month period it lapses and cannot be renewed. The data controller must make a new application. The practice of the OIC is to send a reminder to data controllers before expiry of the entry, although there is no statutory duty to do so. Where a controller pays by direct debit the entry will be automatically renewed as the fee is taken.

Public access to the register

9–34 The Commissioner must provide facilities for making the contents of the register available for inspection free of charge by members of the public at all reasonable hours. This is a mandatory requirement. The register is kept in electronic, not paper, format. In order to fulfill the requirement physical inspection was available by access to a computer terminal connected to the live register at the Commissioner's Wilmslow office; however this no longer appears to be the case. A copy of the register which is updated daily is available over the internet. The Commissioner may also provide such other facilities for making the information contained in the register available free of charge. This is a discretionary power. From August 2012 the copy of the register will be available in a DVD in reusable format as a result of the Open Government initiative.

Certified copies

9–35 The Commissioner must supply certified copies of the particulars contained in the register to any member of the public who requests one. A fee is payable for such a copy. The fee remains £2.

APPLICATIONS FOR REGISTRATION

Method of application

9–36 No particular method of application is prescribed by the Act. There is no requirement in the Act that an application must be in writing. The provision in s.64 that notice in writing is to be taken to include electronic form only applies to notices under Pt II, that is those relating to individual rights. Notification regulations may provide for the registrable particulars to be specified in a particular form. This could be in writing but could equally be used to permit applications to be made in electronic form, whether online or by disk. Applications for notification can be made online and over the telephone as well as by completing a form but in each case the applicant has to sign and return a paper form containing a declaration before the transaction is completed.

Security numbers

9–37 The OIC issues each applicant with a "security number" which should be quoted on any application to alter an entry on the register. This replaces the data user number which was issued under the previous system.

Accuracy of applications

9–38 There is no provision dealing with the accuracy of information to be supplied to the Commissioner. In the 1984 Act, it was an offence to knowingly or recklessly provide false information on an application for registration. Separately, the Registrar had a power to refuse an application on the grounds that the information provided by the applicant was insufficient.

The Registrar took the view that inaccurate information could not be regarded as sufficient and was prepared to refuse applications on such grounds. In the absence of either provision, it appears that the Commissioner would have to accept an entry then take action under s.21(2) if he had sufficient evidence it was false. Section 21(2) makes it an offence for a controller to fail to comply with the duty to keep particulars up to date as required under notification regulations.

Removal of an entry

9–39 The data controller can have an entry in the register removed on application to the OIC as long as he can cite the security number.

Assignment of register entry

9–40 It appears that the benefit of a register entry cannot be assigned or transferred. This is inconvenient where the data controller undergoes a change of legal personality, for example where a sole trader sets up a limited company to carry on the same business the register entry cannot be transferred. The new company must make a fresh application for notification in its own right.

Changes

9–41 In any case where a controller notifies, he must maintain the entry as an accurate record. The extent of the obligation to notify changes, irrespective of whether the notification is voluntary or mandatory, is set out in the Regulations. The purpose is to ensure, so far as is practicable, that at any time the entry contains:

(a) the controller's current name and address; and
(b) a description of the controller's current processing practices or intentions,

and that a description of the current security measures is lodged with the Commissioner. Failure to keep the entry up to date in accordance with the notification regulations is an offence under s.21(2). The offence is one of strict liability although a defence of due diligence is available. Application for changes to the entry must be made in writing and accompanied by the security number. Where the data controller either:

- alters his processing to the extent that the application or entry no longer accurately or completely reflects his activities; or
- changes the security arrangements which he has submitted to the Commissioner;

he must notify the Commissioner of the alteration at the latest within 28 days of its taking place, and amend his entry or statement to reflect the current situation.

Obligations of Commissioner

9–42 A data controller is deemed to be notified from the date on which the correctly completed application form together with the fee is received at the Commissioner's office. If the application is made by registered post or recorded delivery the period of notification begins on the date on which the application was posted. The Commissioner must inform applicants for notification when he has included an entry in the register as soon as practicable and within at least 28 days of receipt of the application. A copy of the entry is sent to the controller when it has been added to the register.

Notification of security provisions

9–43 The 1998 Act requires a data controller to notify the Commissioner of the security arrangements which the controller has in place to protect the personal data. Under s.18(2)(b) a notification must not only specify the registerable particulars in the form determined by or under the regulations but also include "a general description of the measures to be taken for the purpose of complying with the seventh data protection principle".

The seventh data protection principle requires that:

> "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data".

This security information does not appear on the public register. It is held, and presumably assessed or considered, by the Commissioner.

The seventh principle is accompanied by interpretation provisions covering the matters to be taken into account in deciding if security measures are appropriate. Broadly these cover the nature of the data, their possible uses, and the practical and financial impact of achieving effective security for the data including:

(a) standards in handling employees who have access to personal data; and
(b) standards in appointing data processors with access to personal data.

They also require a data controller who is using a processor to process personal data for him to bind the processor by a contract made or evidenced in writing to apply the same standards.

9–44 The security requirements imposed by the seventh principle are thus specified in some detail. However the actual security technique chosen need not be supplied to the Commissioner in that degree of detail. Under s.18(2) the data controller need only supply "a general description" of the security measures.

The Regulations provide that this shall be determined by the Commissioner. These are dealt with by applicants for notification being asked to respond to a list of questions as follows:

> "Do the measures taken by you include
>
> - adopting an information security policy;
> - taking steps to control physical security;
> - putting in place controls on access to information;
> - establishing a business continuity plan;
> - training your staff on security systems and procedures; and
> - detecting and investigating breaches of security when they occur?"

The form previously asked whether the data controller had adopted the ISO Standardon Information Security Management, ISO 17799, but no longer does so. The Commissioner's staff do not assess the level or type of security the controller has in place but simply check that there are some security standards.

ASSESSABLE PROCESSING

Section 22 sets out the power of the Secretary of State to determine the categories of assessable processing for the purposes of the Act. No determination has been made so these provisions have not been activated. Section 22 derives from art.20 of the Directive under which Member States shall: 9–45

> "determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof".

The Directive does not state how the checks are to be done. In the 1998 Act, the checks are to be carried out following receipt of a notification of assessable processing. It might reasonably be assumed that, following those checks, the supervisory authority would have some appropriate range of responses available to it to deal with cases which did show serious risks to individual rights and freedoms, possibly including the imposition of conditions before the start of processing or even forbidding processing altogether in the most extreme case. While this may appear to be the spirit of the Directive, it does not in terms require that any particular powers are to be available to the supervisory authority if a check shows that the processing would cause serious detriment to the rights and freedoms of any individual. Section 22 follows the letter of the Directive. If a notification reveals to the Commissioner that the assessable processing is unlikely to comply with the Act he must inform the controller of his opinion. The Commissioner has no power to forbid the processing or require it to be amended until the controller actually carries it out. The Commissioner will then be able to take enforcement action under his enforcement powers. However, it is possible that by such time the breach may be irretrievable and the damage done.

The assessable processing provisions therefore cannot be used to initiate the Commissioner's enforcement powers. They could be a catalyst for the exercise of individual rights in an appropriate case if the Commissioner were free to inform individuals who are potentially affected by assessable processing of the imminent risks. This would enable such individuals to take injunctive action or lodge notices of objection to the processing in an appropriate case. This seems an unlikely outcome, however, and as it stands s.22 appears to be little more than a formal nod towards the implementation of art.20.

Types of processing

Types of assessable processing may be specified by the Secretary of State by Order. To be specified, processing must appear to him to be particularly likely to: 9–46

(i) cause substantial damage or substantial distress to data subjects; or
(ii) otherwise significantly to prejudice the rights and freedoms of data subjects.

No further assistance is given as to what amounts to substantial damage or substantial distress. It is not clear whether the test is intended to be subjective or objective.

CHAPTER 23

Monitoring Of Communications, Interception And Access To Encrypted Data

INTRODUCTION

23–01 Respect for the confidentiality of communication is a fundamental aspect of the right to privacy as set out in art.8 of the European Convention on Human Rights and Fundamental Freedoms ("the Human Rights Convention"). Article 8 requires the State to respect "private and family life, home and correspondence". Article 5 of Directive 2002/58/EC applies this right to the provision of electronic communications by public service providers. Crucially, art.5 restricts eavesdropping on electronic conversations or monitoring the use of communications systems in public electronic communications systems. In an era in which government security and policing are increasingly reliant on surveillance of all kinds, but particularly surveillance of communications, the scope of the restrictions imposed by art.5 and its predecessor in Directive 97/66 has been a matter of considerable controversy. The importance attached by the Government to surveillance and monitoring of communications for the purposes of tackling crime and terrorism has thrown the impact of these restrictions into sharp relief. The nature of digital surveillance and the proper approach to controlling such surveillance raises many challenging issues. The surveillance techniques to which we are now subject range from CCTV through ANRP to data collected as a result of purchases. In this chapter we only cover the specific areas of:

- the European legal background to the rules governing the monitoring of communications;
- the scope of the European legal instruments;
- the regulation of access to communications data and interception of communications on public telecommunications in the UK under the Regulation of Investigatory Powers Act (RIPA);
- the regulation of access to encryption keys in the UK under the RIPA; and
- the regulation of the interception of communications on private systems under the Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 ("LBP Regulations") made under RIPA.

In addition to access to communications data and the interception of communications on public networks, RIPA covers covert surveillance, use of

intelligence sources and related matters. Only Pt 1 of Ch.I—Unlawful and authorised interception, Ch.2—Acquisition and Disclosure of Communications Data, and Pt III—Investigation of electronic data protected by encryption, are covered in this chapter.

The scope of the European legal instruments is important in this context as it affects how much freedom the UK has to decide on its own rules in some of these areas. The relationship with the European legal instruments is therefore considered. Note that the overall scheme for the regulation of electronic communications is outlined in Ch.22.

BACKGROUND

23–02 The rules which govern this area are derived from supra-national legal instruments: the Human Rights Convention, Directive 2002/58 and its predecessor Directive 1997/66. There were deficiencies in the way that the UK implemented its obligations under these instruments which are noted in the text and action was taken in relation to deficiencies which came to the attention of the Commission as a result of the Phorm Webwise issue in 2008. This resulted in amendments to RIPA covered below. There are different rules for interception of communications and for access to communications data. Interception has a legal definition in the Regulation of Investigatory Powers Act 2000 (RIPA) but broadly covers any access to the content of communications. Interception may take place either by monitoring, that is listening into a conversation in the course of its transmission across a communications network[1] or viewing an e-mail exchange while it is taking place; or recording, that is accessing the communication message in the course of its transmission across a communications network and taking a copy to listen to or read later. Access to communications data means having access to the traffic data about the communication, including the service data and subscriber data.[2]

Communications data is the information generated as a result of electronic communications (such as the number called or the length of the call) rather than the content of the communication. There are special rules which allow businesses (which includes the public sector for these purposes) to intercept the contents of communications on their own systems subject to safeguards. These are found in the LBP Regulations. There are no provisions which specifically authorise businesses (including the public sector) to access or use the communications data on their systems.

[1] Note that monitoring one half (or even both halves) of a conversation via bugging devices would not constitute an interception: see, e.g., *R. v Smart* [2002] EWCA Crim 722 at para.68.
[2] See s.21(4)(b) and (c) of RIPA. Schs 1 and 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) set out which public bodies have access to which types of communications data; many only have access to service data not traffic or subscriber data.

SUMMARY OF MAIN POINTS 23–03

(a) Interception of communications and access to communications data involve breaches of art.8 of the Convention rights and on public networks are subject to art.5 of Directive 2002/58.
(b) Interception, access to communications data and retention of communications data are covered by a number of intersecting provisions.
(c) Public bodies carrying out interception of content on private electronic communications systems which they control (e.g. internal government department systems) are subject to art.8 of the Convention and have a lawful basis for their interference with those rights as long as they comply with the LBP Regulations.
(d) Private bodies carrying out interception of content on private electronic communications systems (e.g. internal telephone systems) are not directly subject to art.8 of the Convention but in any event have a lawful basis for the interception as long as they comply with the LBP Regulations.
(e) Public or private bodies carrying out surveillance of or accessing communications data on private electronic communications systems which they control (e.g. internal systems) have no clear legal basis for the interference as the LBP regulations do not cover communications data and the legal position of such surveillance or access is uncertain.
(f) Public bodies carrying out interception or access to communications data on public telecommunications systems are subject to art.8 of the Convention and art.5 of Directive 2002/58 and have a lawful basis for their interference with those rights as long as they have proper authority under RIPA, e.g. warrants.
(g) There is no lawful basis for private organisations to be authorised to carry out interception or access communications data on or from public telecommunications systems. Any such interception or access carried out intentionally would be unlawful under RIPA unless those subject to the interception or access gave consent.

BACKGROUND

Article 8 of the Convention rights

The interception or surveillance of a communication is clearly an interference with the art.8 right of an individual.[3] Article 8 provides: 23–04

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or he

[3] See Ch.2 for a full description of the impact of the HRA and the case law on art.8 since October 2000. Concerns about the impact of interception on private life were expressed by the Article 29 Working Party in its Recommendations in the Respect of Privacy in the Context of Interceptions of Telecommunications of May 3, 1999.

> democratic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

This is now part of UK law by virtue of the Human Rights Act 1998. In the past the UK was found wanting before the European Court of Human Rights because of its failure to regulate comprehensively the interception of communications. The first statute to regulate the interception of communications was the Interception of Communications Act 1985 (IOCA), which was passed following an adverse finding against the UK in the case of *Malone v UK*.[4] UK practice had been for telephone taps to be carried out under administrative practices with no comprehensive statutory code governing surveillance activities. Thus the practice did not comply with the standards necessary to meet art.8(2) as it was not set out in a legal scheme which was sufficiently clear or transparent to enable the citizen to understand in what circumstances and in what conditions public authorities were empowered to carry out such activities.[5]

IOCA made it an offence to intentionally intercept a communication in the course of transmission by a public telecommunications system, unless either it was done with the authority of a warrant issued by the Secretary of State or the interceptor had reasonable grounds for believing that either the sender or the recipient had consented to the interception. However, the limited remit of IOCA meant that the UK continued to face adverse findings by the Court at Strasbourg in relation to interception. In the case of *Halford v United Kingdom*,[6] the Court found that the tapping of a telephone which was part of a private network was not covered by IOCA and thus without a proper legal basis. In a variety of cases the Court also found that the failure by the UK to regulate surveillance by electronic eavesdropping in other ways breached art.8.[7] In the UK courts in *R. v Effick*[8] it was held that calls from a cordless telephone which were intercepted between the base unit and the telephone were not covered by IOCA.

23–05 When the Convention rights were implemented in the United Kingdom by the HRA it was imperative that the entire area of surveillance was reviewed and put on to a proper statutory footing. The government decided that the appropriate approach was to deal with both art.5 of Directive 97/66 and art.8(2) of the Convention rights in the same legislation and did so in RIPA and the LBP Regulations.

Article 5 of Directive 97/66 and 2002/58

23–06 Article 5(1) of Directive 2002/58 requires Member States to ensure the confidentiality of

> ". . . communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, except with the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)."

[4] (1985) E.H.R.R. 14.
[5] For a more detailed analysis see K. Starmer, *European Human Rights Law.*
[6] (1997) 24 E.H.R.R. 523.
[7] *Khan v United Kingdom* (2001) 31 E.H.R.R. 45; *PG v United Kingdom* [2002] Crim. L.R. 308.
[8] [1994] 3 All E.R. 458.

In 2010 the UK was found to have failed to have implemented the requirement properly and made consequential amendments to RIPA in 2011, which are covered below. The provision largely re-states art.5 of Directive 1997/66; the difference is in the addition of the reference to "and related traffic data" which is dealt with below. However, in respect of the interception of the content of communications the provision is identical. It requires Member States to prohibit the interception of communications and access to communication data on public networks except either where users of the communication system have consented or the interception is legally authorised.

The scope of areas where legal authority may permit an interference is not in fact limited to the derogations provided for by art.15(1), as art.5(2) further provides that:

> "(2) Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purposes of providing evidence of a commercial transaction or of any other business communication"

Recital 23 provides some further explanation of the scope of this derogation as follows:

> "Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purposes and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged".

23–07 The derogations provided for by art.15(1) permit Member States to adopt legislative measures to restrict the scope of the rights and obligations where the restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard

> ". . . national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system."

The judgment of the Court of Justice of the European Union (CJEU) in *Productores de Música de España (Promusicae) v Telefónica de España SAU* (C-275/06) made clear that the grounds of exemption allowed in 95/46/EC should also be regarded as relevant to 2002/58. Article 15(1) makes it explicit that Member States may adopt laws to provide for the interception of communications including cases where the reasons fall outside community competence but the measures must be in limited to those allowed by the Article. Any abrogation of the confidentiality of communications must also be in accord with Community

law including the principles in art.6(1) and (2) of the Treaty. The principles in art.6(1) and (2) enshrine the fact that the Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms.[9]

Directive 2002/58 does not apply to areas outside the scope of EU law and thus interception may take place for matters outside scope. Recital 11 of 2002/58 makes this point explicit but also makes it explicit that the Convention rights continue to apply to such interception. RIPA is primary legislation and its provisions apply to all interception which is within its scope.

Confidentiality of communications data

23–08 As noted above, Directive 97/66 did not impose any restriction on the access to communications data. It did impose restrictions on how such data can be used by those who provide public electronic services which have now been repeated in Directive 2002/58 and are implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulation 2003 (see Ch.22). Directive 2002/58 placed access to communications data arising from public electronic communications services on the same footing and subject to the same restrictions as interception. There has however been no subsequent change to the relevant statutory provisions in RIPA or the LBP Regulations.

RIPA covers the acquisition and disclosure of communications data by designated public authorities from public service providers and operators of private systems, such as those used internally in business and public offices. The LBP Regulations do not deal explicitly with communications data. The current situation therefore is that operators of private networks, both public and private sector, access and use communications data for their own purposes such as HR management without any general supervisory regime other than the data protection principles; specifically there is no legal basis for accessing such data. It can be assumed that the view of the UK Government was that operators of private systems, whether the system controller is in the public or the private sector, need no additional powers to access or use communications data. The case of *Copland*,[10] however, suggests that such use and access, by public bodies at least, engages art.8 of the Convention Rights

Copland v United Kingdom

23–09 Mrs Copland was employed by a Further Education College. During the course of her employment her telephone and internet useage were monitored by her employer. There was some dispute over whether interception of contents took place but the Court took the view that it did not have to decide that as the monitoring of the communications data amounted to a breach of art.8 in any event. Mrs Copland had not been told that her communications would be monitored. The UK government had argued that the monitoring of the communications data did not amount to an interference in private life but the Court held that it did. The Government also argued that, if there was an interference, it was on lawful grounds, being incidental to the powers of the

[9] art.15(1).

[10] Application No.62617/00.

college and was proportionate. The Court held that there was no lawful basis as there was no express power and therefore the question of proportionality did not arise. It found against the UK on art.8 and also art.13 in that Mrs Copland did not have an effective remedy for the breach of her art.8 rights. It appears that the UK Government dealt with the judgment by stating to the Joint Committee on Human Rights in 2007 that it had implemented the Court's judgment in Copland by virtue of Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and that this was accepted by the Committee of Ministers in March 2008.[11] However, the response did not deal specifically with communications data and although it has been accepted by the Committee of Ministers the result seems open to doubt as the Regulations do not cover communications data.

COVERAGE OF DIRECTIVES

Areas which are outside Community competence are outside the remit of Community law. Article 3(2) of Directive 95/46/EC specifically sets out those limits by providing that the Directive does not apply to the processing of personal data carried out in the course of activities which fall outside the scope of Community law and explicitly not to processing operations 23–10

> "concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in the areas of criminal law".

A directive itself may also be limited in scope because of the basis on which it was made. Directives are secondary legislation of the Community. A legal basis for the making of a directive must be found in the Treaties.[12] Directive 95/46/EC was made as an internal market measure on the basis of art.95. Any purported action under the Directive must fall within the scope of art.95.

The limitations of the legal basis were emphasised by the ruling of the European Court of Justice in the cases heard on the transmission of Passenger Name records (PNR) to the United States.[13] Following the terrorist attacks of November 9, 2001 the United States had required airlines to disclose detailed passenger information relating to those who travelled to the country. In order to provide a lawful basis for the required disclosures the European Commission had adopted two decisions, the first holding that the US Bureau of Customs and Border Protection (CBP), part of the Department of Homeland Security, provided a sufficient level of protection for the personal data being transferred and the other embodying an agreement with the US authorising the transfers.[14] The 23–11

[11] *http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/173/17317.htm* [Accessed October 5, 2012].

[12] For a fuller discussion of the scope of Community law, see Ch.1, paras 1-16 onwards.

[13] Joined Cases C-317/04 and C-318/04 of the European Court of Justice, May 30, 2006.

[14] Commission decision 2004/535/EC of May 14, 2004 on the adequate protection of personal data contained in Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection ([2004]OJ L235 p.11) and Council Decision 2004/496/EC of May 17, 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States of America

European Parliament applied for the decisions to be annulled on the basis that the decisions were outwith the competence of the Council and the Commission.

Community competence

23–12 The institutions of the Community do not have competence to rule on matters that are not within the Treaties of the Union. Security is outside the scope of Community competence. The agreement with the US on PNR was for the purposes of security and thus the Commission and the Council were not able to make binding instruments in relation to it. The European Court agreed with the Parliament and the Decisions were annulled with effect from September 30, 2006.[15]

A Member State is not required by EU law to apply a provision of a Community instrument, such as a directive, to an activity outside an area of Community competence, although the Member State may chose to apply the standards required by a directive to all areas of relevant behaviour by national law. When implementing the data protection directives the UK had a choice as to how it would implement. It could have implemented by secondary legislation and made regulations under the European Communities Act 1972. Regulations can be made under this Act only in relation to areas falling within Community competence. Alternatively it could pass primary legislation. The United Kingdom elected to pass primary legislation, making the Data Protection Act 1998 generally applicable national law, including those areas which are not covered by Community competence.

Directives 1997/66 and 2002/58 however were implemented by regulations made under the European Communities Act 1972 and are therefore only applicable to areas covered by Community competence.

Directive 2002/58 applies, and will be relevant as an aid to interpretation, where the surveillance or interception falls within areas of Community competence, as with the monitoring of business calls, but does not apply, and is only persuasive, at best, when the surveillance or interception is carried out for purposes outside Community competence such as national security. It should be noted, however, that art.5 (see para.23-07, above) of the predecessor Directive was implemented by primary legislation, RIPA. The LBP Regulations are made under that primary legislation. RIPA will therefore apply irrespective of the rules relating to Community competence. The tortuous relationship between the two is recognised in reg.3(3) of the LBP Regulations, which provides that interception or monitoring falling within certain grounds (those in para.1(i)(a), that is those which relate to ordinary business use) are only authorised to the extent permitted by art.5. Implicitly, therefore, monitoring for other purposes, which cover areas such as national security which are outside Community competence, may exceed the remit of art.5 as Directive 2002/58 is irrelevant to those areas. Nevertheless, such activities will still be covered by RIPA 2000 and the DPA 98, which are both primary legislation of general application in the UK.

on the transfer and processing of PNR data by Air Carriers to the United States Department of Homeland security, Bureau of Customs and Border Protection ([2004] OJ L183 p.83).

[15] For a more detailed review, see Ch.1, paras 1-16 onwards.

This is relevant to the issues raised by the debate on the retention of traffic data as well as to the surveillance debate. Where art.8 of the Convention rights applies, however, interception, and now it appears following *Copland,* access to and use of communications data, must comply with art.8(2) of the Convention rights.

SCOPE OF CONVENTION RIGHTS

23–13 The Human Rights Convention and the HRA are only directly binding on public authorities. In some circumstances the ECtHR has held that the State has an obligation to ensure the protection of rights against the actions of another private person. The Court has said that this applies to art.8. The extent of the obligation is unclear. The courts in the UK have taken account of art.8 in the law as it is applied to private bodies such as the media in respect of the publication of information since the HRA came into effect in 2000.[16] It is possible, therefore, that the art.8 right could influence decisions in respect of private bodies, for example by influencing the interpretation of employment laws. In *McGowan v Scottish Water*[17] the EAT considered the application of art.8 in an employment case. The employer however was a public authority. In that case the EAT upheld the ruling of the Tribunal that covert surveillance of an employee's house was not a breach but if it was a breach it was justified.

As far as public bodies are concerned they are bound by art.8 of the Convention rights but they have no mechanism for obtaining authorisation for the monitoring of communications data generated by internal systems. Public bodies are only able to apply for authorisation for interception or access to communications data under the relevant provisions of RIPA for the purpose of their public functions. This point was made clear in the case of *C v Police and Secretary of State for the Home Department.*[18]

C v Police and Secretary of State for the Home Department[19]

23–14 The Investigatory Powers Tribunal has exclusive jurisdiction to hear complaints about the misuse of powers relating to surveillance authorised or carried out under RIPA. A retired police officer complained to the Tribunal that he had been subject to covert surveillance by private investigators acting for the police force. The complainant had taken early retirement on medical grounds. He had been awarded compensation and an "enhanced injury" award after tripping over a carpet in a police station. The force wished to check the extent of the injuries he had suffered. The complainant asserted that the surveillance should have been authorised under the provisions of s.26 of RIPA. This provides for the authorisation of planned covert surveillance which is not intrusive; is carried out "for the purpose of a specific investigation or specific operation", and will result in the obtaining of private information about a person.

[16] See Ch.2 for the cases on privacy and the media decided since October 2000.

[17] UKEAT/007/04

[18] Investigatory Powers Tribunal, No.IPT/03/32/H, November 14, 2006.

[19] Investigatory Powers Tribunal, No.IPT/03/32/H, November 14, 2006.

23–15 The case hinged on whether the surveillance by a public authority for a private law purpose such as employment-related matters was covered by s.26. The Tribunal held that it was not and that only surveillance for the purposes of the investigatory functions of public bodies can be authorised and carried out under RIPA. Accordingly the claimant had to bring his claim within the general law, applying art.8 and data protection and privacy rights, rather than having any remedy before the specialist tribunal.

As part of its judgment the Tribunal made some general comments on the nature of surveillance, the taking of photographs and the obtaining of information more generally:

> "Surveillance by public authorities (or indeed anyone else) is not in itself unlawful at common law, nor does it necessarily engage Article 8 of the Convention. For example, general observation of members of the public by the police in the course of carrying out their routine public duties to detect crime and to enforce the law is lawful. It does not interfere with the privacy of the individual citizen in a way that requires specific justification; see, for example, Friedl v Austria (1995 21 EHRR)".

This should now be treated with some caution given the ECtHR and UK case law on the taking and use of photographs. In Wood v Commissioner for Police of the Metropolis,[2009] EWCA Civ 414. the Court of Appeal, by a two to one majority, decided that the Metropolitan Police had acted unlawfully when it retained photographs which it had taken of an anti-arms trade campaigner as he was leaving the AGM of Reed Elsevier Plc ("REP"). Although the police were justified in taking the photographs in the first instance the court said that they should have been destroyed after a short space of time once it was realised that they were not needed.[20]

REGULATION OF INVESTIGATORY POWERS ACT 2000

Communications data

23–16 Communications data under RIPA covers traffic data under Directive 2002/58 but is a wider definition. Chapter II makes provision for authorised persons to obtain communications data from telecommunication operators subject to service of appropriate notices and places operators under obligations to make disclosures. However, it imposes no obligation on operators to retain data for any specific length of time, a point which caused problems for both operators and authorities as the prohibition in Directives 97/66 and 2002/58 on the retention of traffic data was opposed to the wishes of the investigation and intelligence communities to have widespread access to such data accumulated over significant periods. This has now been addressed, at least in part, in the rules governing the retention of communications data (see Ch.24). It should be noted for completeness that access to communications data may not be sought exclusively under RIPA. There are

[20] See Ch.6 for the case law on photography.

numerous statutes which pre-date RIPA but which would also potentially allow for the relevant public body to seek such information for the purposes of their functions.[21]

Definition of communications data

23–17 This is defined as:

> "(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted;
>
> (b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—of any postal service or telecommunications service; or in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunications system;
>
> (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".[22]

The contents of any communication are not included in the definition. Traffic data is defined in relation to any communication as:

> "(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
>
> (b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
>
> (c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and
>
> (d) any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer programme access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored".[23]

It appears from the breadth of the definition that cookies would be capable of being communications data. If that is the case then, under Directive 2002/58, an employer who reviews the cookies on the system to see which websites have been visited by employees would be accessing communications data.

23–18 It is further provided that traffic data includes any references to the actual apparatus through which it is transmitted.[24]

Chapter II applies to conduct in relation to a postal service or telecommunications service for obtaining communications data other than conduct consisting in

[21] See *Freedom from Suspicions—Surveillance reform for a digital age*, para.153, quoting Lord MacDonald in *Review of Counter Terrorism and Security Powers*(Com 8003, January 2011).

[22] s.21(4).

[23] s.21(5).

[24] s.21(7).

the interception of communications in the course of their transmission by means of such a service or system and the disclosure to any person of communications data.

It provides that conduct to which the Chapter applies shall be lawful where it is conducted by an authorised person in accordance with the authorisation.[25] As noted earlier however it makes no provision for establishing the lawfulness of access to and use of communications data other than under Ch.II.

It provides for designated persons to serve notice on postal or telecommunications service operators requiring the operator to disclose specified communications data[26] and places a duty on the service providers to comply with the requirements of the notice[27] as far as is reasonably practicable.[28] If the operator does not already have the data in his possession the notice may require him to obtain it, if the operator is capable of doing so. The obligation on the operator may be enforced by civil proceedings for an injunction by the Secretary of State "or other appropriate relief".[29]

The designated person must believe that it is necessary to obtain the communications data for one of the specified interests or purposes and that it is proportionate to the objective to be achieved that the data be obtained.

Specified interests or purposes

23–19 These are partially set out in reg.22(2), but the list is not exhaustive as it includes a provision for the Secretary of State to specify further purposes by order. There has been one order under this provision.[30] The purposes provided for in the sub-section are:

- the interests of national security;
- the purpose of preventing or detecting crime or of preventing disorder;
- the interests of the economic well-being of the United Kingdom;
- the purpose of protecting public health;
- the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist in investigations into alleged miscarriages of justice; and
- to identify and notify the next of kin of a deceased or incapable person.

The categories of designated persons are officials or office holders for public authorities as listed or as prescribed by the Secretary of State.[31] Such persons are then entitled to authorise others of the same level or rank to exercise the powers.

[25] Regulation of Investigatory Powers Act 2000 s.21(1).
[26] s.22(4).
[27] s.22(6).
[28] s.22(7).
[29] s.22(8).
[30] The Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 (SI 2006/1878), replaced by SI 2010/480.
[31] Regulation of Investigatory Powers Act 2000 s.25(2).

All authorisations and notices must be given in writing and contain prescribed particulars.[32] A notice may have effect for a month but may be renewed. Notices may also be cancelled. The Secretary of State may make arrangements for contributing to the cost of complying with notices under these provisions.

These provisions potentially allow officials of public authorities widespread powers to serve notices requiring communications data with no other authorisation. The Home Secretary brought out a draft order under s.25(2) in June 2002, which listed a wide range of public authorities including government departments, local authorities, fire authorities and others as prescribed authorities. The draft met with stiff opposition and was withdrawn by the Government.[33] It was replaced by a narrower list under which access to all categories of communications data was restricted to broadly policing and associated organisations while other public bodies have access to only a sub-set of the possible categories of communications data. The number of bodies with access was extended by subsequent orders until in 2007[34] a total of 795 public bodies were able to request some level of communications data.[35] The use of communications data by some public bodies has been widely criticised, for example a local authority using the powers to check whether a family were using schools to which they were not entitled because they did not live in the catchment area.[36] As a result the Government issued a further consultation in April 2009. This resulted in the replacement of the previous Orders by one consolidated Order which sets out the additional purposes for which access to the data can be granted and lists the organisations and individual authorised to seek access.[37] The response did not satisfy critics. The criticisms of the provisions are not only directed at the number of bodies that may access communications data but the absence of an independent authorisation process. The Coalition programme for government included a commitment to address problems with RIPA and the Protection of Freedoms Act 2012 includes a provision requiring judicial sanction before allowing local authority access to communications data. This now appears as ss.23A and 23B of RIPA as inserted by s.37 of the 2012 Act.

23–20 The term operator simply means a person who provides a telecommunications service. Therefore notices can be served on those who provide services other than as a public telecommunications service, such as providers of private systems in hotels or businesses.

Codes of practice

23–21 The provisions relating to codes are found in ss.71 and 72. Section 71 provides (inter alia) that the Secretary of State must issue one or more codes of practice relating to the exercise and performance of the powers and duties under Pts I–III

[32] Regulation of Investigatory Powers Act 2000 s.23(1) and (2).
[33] See the website for the Foundation for Information Policy research (*www.fipr.org* [Accessed October 5, 2012]) for relevant press releases.
[34] The Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172) amended by the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Orders 2005 (SI 2007/1083) and 2006 (SI 2006/1878).
[35] Report of the Interception Commissioner.
[36] Poole Borough Council, reported by BBC, April 2010.
[37] The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480).