Protection of Employees' Personal Information and Privacy in English Law

Gillian Morris
University College London

1. Introduction

1.1 The protection of employees' personal information and privacy has become an important area of debate in the light of technological developments which allow much greater scope for employers to monitor the activities of their workers both in and outside work. The problem is exacerbated by the blurring of the work/home divide as new technology permits workers to perform many roles away from the traditional workplace. One particular area of controversy in Britain has been the practice of employers examining the social media profiles of job applicants in order to vet them for inappropriate language or behaviour, sometimes demanding passwords or to be a social media 'friend' in order to access these profiles.[1] Until fairly recently many people seemed unaware of the potential implications for employment of their social media profiles[2] although the press publicity this has received may change behaviour. However the high profile lawsuits have focussed on the rather different issue of those who have disparaged their employers or their colleagues on-line, or revealed work-related misconduct such as feigning illness, and have been disciplined as a consequence.

1.2 The relative absence of litigation relating to the protection of employees' personal information may be due in part to the complexity and weakness of the law. As this paper shows, English law in this area is fragmented and offers inadequate protection in the employment sphere in many important respects

1.3 The paper begins by outlining the regulatory framework for the protection of employees' personal information and privacy. It then examines the purposes for which obtaining employees' personal information and monitoring their activities may be seen as appropriate and reasonable and how English law strikes a balance between business necessity and employees' privacy protection. There follows an analysis of the specific protections which apply during the hiring process; employment relationship; and following termination of that relationship. The concluding section evaluates the effectiveness of the current regulatory provisions and makes some proposals for reform.

[1] The term 'Britain' refers to England, Wales and Scotland. As Scottish law differs in some material respects from the law of England and Wales this paper deals specifically with 'English' law.
[2] A. Broughton, T. Higgins, B. Hicks and A. Cox *Workplaces and Social Networking: The Implications for Employment Relations*, Acas, 2010: p 22.

2. The Regulatory Framework

2.1 There is no single, comprehensive piece of legislation in England which regulates the protection of employee's personal information and privacy; rather the relevant law is derived from several different sources, some specific to the employment context, some of wider application. These sources are as follows:

(a) Human rights treaties and legislation
(b) Data protection legislation
(c) Legislation on the interception of communications
(d) Legislation on access to medical reports
(e) Legislation on information about criminal offences
(f) Equality legislation
(g) The common law.

This section provides a brief outline of the scope of protection afforded by each of these sources, together with the mechanisms of enforcement and remedies. Greater detail about the application of these provisions to particular stages of the employment relationship is given later in the paper. There are two recurring issues which it is appropriate to highlight at the outset, however. The first is the relevance of an individual's 'consent' in relation to the collection of personal information by employers under many of these provisions. The extent to which individuals are adequately protected in the event that they refuse consent or challenge whether the employer has the right to specified information is discussed in the concluding section of the paper. The second issue is that of the remedies available to the individual where the law is breached, which are not well-suited to the employment context.

Human rights treaties and legislation

2.2 The UK is a signatory to the *European Convention on Human Rights* ('ECHR') , Article 8 of which provides that:

> (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 the law and is necessary in a democratic society in the interests of national security, public safety or the economic 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. [3]

2.3 The European Court of Human Rights ('ECtHR') has made clear that 'private life' is not confined to the 'inner circle' in which individuals live but that it must 'comprise to a certain degree the right to establish and develop relationships with other human beings', a notion which extends to activities of a professional and business nature given that it is 'in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world'.[4] It is also clear that personal communications to and from business premises, including telephone calls, e-mails and information derived from monitoring internet usage, fall

[3] See also the Charter of Fundamental Rights of the European Union (2010), articles 7 (respect for private and family life) and 8 (protection of personal data).
[4] *Niemietz* v *Germany* judgment of 16 December 1992, (1993) 16 EHRR 97, para 29.

within Article 8.[5] One important question is the extent to which the scope of the right to respect for private life can be shaped by the employment contract; there is some support in the cases for the view that a worker's expectation of privacy may be removed by agreement between the parties, or possibly even by a warning on the part of the employer, so allowing the employer unilaterally to define the 'private' zone.[6] However in other cases (outside the employment field) the court has emphasised that 'a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor'.[7] A more transparent approach than permitting the scope of the right to respect for private life to be limited by contract or a warning, and one consistent with its status as a fundamental right, is to require any interference to be justified under Article 8(2).[8] It is also possible that some more extreme forms of interference with a worker's private life, such as surveillance of staff toilets, could be regarded as 'degrading treatment', contrary to Article 3 of the ECHR, which cannot be justified in any circumstances.

2.4 If the ECtHR finds that a right protected by the ECHR has been violated and the internal law of the respondent state allows only partial reparation to be made the Court may award 'just satisfaction' to the injured party which may include awards for both pecuniary and non-pecuniary loss, such as the stress and anxiety caused by the interference with the right.[9] The Court has held that the State's obligations under Article 8 are not confined to abstention from interference but 'may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves.' [10]

2.5 The *Human Rights Act* ('HRA') 1998 gives 'further effect' in the UK to rights and freedoms guaranteed under the ECHR. Article 8 has an impact on English law in three major ways:

(a) The HRA requires all legislation (whenever passed) to be 'read and given effect in a way which is compatible' with 'the Convention rights' '[s]o far as it is possible to do so'.[11] Article 8 may, therefore, influence the interpretion given to the legislation discussed below.[12] If primary legislation cannot be read compatibly with a Convention right (or, in the case of subordinate legislation which is incompatible, the primary legislation prevents removal of the incompatibility) a court may make a 'declaration of incompatibility'.[13] This

[5] *Copland* v *UK* judgment of 3 April 2007, (2007) EHRR 37, para 41.
[6] *Halford* v *UK* judgment of 25 June 1997, (1997) 24 EHRR 523, para 45; *Copland* v *UK*, above, para 42.
[7] *PG and JH* v *UK* judgment of 25 September 2001, (2001) ECHR 550.
[8] See generally G.S. Morris 'Fundamental Rights: Exclusion by Agreement?' 30 *Industrial Law Journal* 49. For a recent review of ECHR case law see Frank Hendrickx and Aline van Bever 'Article 8 ECHR: Judicial Patterns of Employment Privacy Protection' in *The European Convention on Human Rights and the Employment Relation* ed F Dorssemont, K Lörcher and I Schömann, 2013.
[9] See *Copland* v *UK*, above, note 5, for an example of an award for non-pecuniary damage in the employment context.
[10] *X and Y* v *The Netherlands* judgment of 26 March 1985, (1985) ECHR 4. See *Köpke* v *Germany* judgment of 5 October 2010, [2010] ECHR 1725 on the State's positive obligation relating to video surveillance of workers.
[11] HRA 1998, s 3.
[12] For a recent example of Article 8 arguments being used to influence the interpretation of the Data Protection Act 1998 see *Vidal-Hall and others* v *Google Inc* [2014] EWHC 13 (QB), [83]-[103].
[13] HRA 1998, s 4. For limits to the capacity to read legislation compatibly with Convention rights see *Ghaiden* v *Godin-Mendoza* [2004] UKHL 30.

does not affect the continuing validity of the offending legislation but a special 'fast-track' procedure may be used to amend it.[14]
(b) The Act makes it unlawful for a 'public authority' (including a court or tribunal) to act in a way which is incompatible with a Convention right unless, as a result of the provisions of primary legislation, it could not have acted differently. 'Victims' of such acts may bring proceedings against a public authority, or rely upon Convention rights in any other proceedings. Thus, workers employed by 'public authorities' who allege that their employer has violated their rights under Article 8 may bring proceedings directly against them; if it upholds the claim the court may grant such remedy within its powers as it considers 'just and appropriate', taking into account, if it decides to award damages, the principles applied by the ECtHR.[15]
(c) The application to courts of the duty not to act unlawfully in (b) above has been interpreted to mean that Convention rights should be taken into account in common law proceedings, regardless of the legal identity of the claimant or defendant. Article 8 has been highly instrumental in recent cases relating to breach of confidence to provide a remedy for unauthorised disclosure of private information and although there is as yet no tort of breach of privacy *per se* there is some judicial support for a tort of misuse of private information.[16] The requirement for courts and tribunals not to act incompatibly with Convention rights may also be material in interpreting the contract of employment. There is a strong argument that employees should not be required to obey instructions which breach their Article 8 rights and that conduct by an employer that breached those rights would breach the implied contractual duty of trust and confidence.[17]

Data protection legislation

2.6 The *Data Protection Act* ('DPA') 1998 was enacted to implement EC Directive 95/46 on personal data. All those who determine the purposes for, and manner in, which 'personal data' is to be 'processed' ('data controllers') have obligations under the DPA; the Act therefore is capable of covering, but is not confined to, employers. The term 'data' does not include all the information which employers may obtain about their workers, however. It covers information which is 'being processed by means of equipment operating automatically in response to instructions given for that purpose', is recorded with the intention of being processed by such means; or 'is recorded as part of a relevant filing system or with the intention that it should form part of' such a system'. A 'relevant filing system' means 'any set of information relating to individuals' to the extent that 'the set is structured … in such a way that specific information relating to a particular individual is readily accessible'.[18] The English courts have held that manual records are covered only if they are of 'sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system', requiring a filing system so referenced or indexed that it

[14] HRA 1998, s 10.
[15] As above, ss 6-8. There is voluminous case law and academic literature on the meaning of 'public authority'. As this is of little relevance to the subject-matter of this paper it is not explored further here.
[16] See *Campbell* v *MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *OBG Ltd* v *Allen and Douglas v Hello!* [2008] 1 AC 1 and other cases cited in *Vidal-Hall,* above, note 11. For a sceptical view of the impact of the HRA 1998 on the common law in general see Jane Wright, 'A Damp Squib? The Impact of Section 6 HRA on the Common Law: Horizontal Effect and Beyond' [2014] *Public Law* 289.
[17] See S. Deakin and G.S. Morris, *Labour Law* 6th edn, 2012, paras 4.105-4.107 for this duty.
[18] Data Protection Act 1998, s 1. Information forming part of an 'accessible record' as defined by s 68 is also covered, as is recorded information held by a public authority.

enables the data controller's employee 'to identify at the outset of his search with reasonable certainty and speed the file or files in which the specific data relating to the person requesting the information is located … without having to make a manual search of them'.[19] This approach focusses, therefore, on the method of recording information and the ease with which it can be found rather than its sensitivity or importance to the individual worker and constitutes a major gap in data protection.[20] 'Personal data' means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession, or likely to come into the possession, of the data controller; also included is any expression of opinion about, and any indication of the intentions of any person in respect of, the individual.[21] The 'processing' of data is widely defined to cover 'obtaining, recording or holding the information or data or carrying out any operation or set of operations' on it; this specifically includes retrieving, consulting, using, erasing or destroying data.[22]

2.7 'Data controllers' must comply with eight 'data protection principles' in respect of personal data.[23] Those of greatest relevance to protection of personal information in the employment context are as follows:

(a) The duty to process data 'fairly and lawfully' (the 'first principle'). This duty requires the data subject to consent to the processing or one of a number of other conditions, discussed in paragraph 3.2 below, to be met. An additional condition (including 'explicit consent')[24] must be met in the case of 'sensitive personal data', defined as information as to the racial or ethnic origin of the data subject; his or her political opinions, religious beliefs or other beliefs of a similar nature; whether he or she is a member of a trade union; his or her physical or mental health or condition or sexual life; or the commission or alleged commission of a criminal offence or any proceedings for any such offence, the disposal of such proceedings or the sentence of the court.[25] The employer must ensure so far as practicable that the data subject is provided with, or has readily available to him or her, specified information, including the purposes for which the data are intended to be processed and any further information which is necessary in the circumstances to enable processing to be fair.[26]

(b) Personal data must be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes (the 'second principle').

(c) Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed (the 'third principle').

---

[19] *Durant* v *Financial Services Authority* [2004] FSR 28, Auld LJ at [48]. The 'property rights' of data controllers, who were allowed only a limited time to respond to requests for information and entitled only to a limited fee (see para 5.11 below), weighed heavily with the Court of Appeal.

[20] The Information Commissioner (see para 2.8 below) considers that the system 'must amount to more than a bundle of documents about each worker filed in date order' and that a personnel file with nothing to guide a searcher to where specific information such as the worker's leave entitlement can be found is unlikely to be covered by the DPA 1998: *Employment Practices Data Protection Code* (2005).

[21] DPA 1998, s 1.

[22] As above.

[23] DPA 1998, s 4; Scheds 1-3.

[24] See para 7.2 below for discussion of 'consent' and 'explicit consent'.

[25] DPA 1998, s 2.

[26] DPA 1998, Sched 1, Part II.

(d) Personal data must be accurate and, where necessary, kept up to date (the 'fourth principle').
(d) Personal data processed for any purposes must not be kept for longer than is necessary for those purposes (the 'fifth principle').
(e) Personal data must be processed in accordance with the rights of data subjects under the Act (the 'sixth principle'), such as the rights to be supplied with information on request or to require, in specified conditions, that the employer should cease processing the data (see paragraph 5.11 below).

2.8 The DPA 1998 provides for the appointment of an 'Information Commissioner' who performs various duties under the Act, including publishing codes of practice.[27] Published codes include an Employment Practices Data Protection Code (the 'EPDPC') which makes recommendations on recruitment, employment records, monitoring at work, and information relating to workers' health. These codes are not legally binding but are likely to be cited by the Commissioner in connection with any enforcement action taken by him.

2.9 The Information Commissioner is obliged to make an assessment as to whether it is likely that processing is being carried out in accordance with the DPA 1998 at the request of the person directly affected or another person acting on his or her behalf.[28] The Commissioner can also make a range of orders to enforce the Act.[29] The main ones potentially relevant to employment are information notices;[30] enforcement notices;[31] and monetary penalty notices (up to a maximum of £500,000).[32] In addition the DPA creates a number of specific criminal offences, including failing to register as a data controller with the Information Commissioner and breaching the 'enforced subject access' prohibition described in paragraph 4.2 below. Finally, an individual who suffers damage by reason of any contravention of the DPA 1998 is entitled to compensation for that damage, although the data controller can defend the action by proving that he or she had taken all reasonable care to comply with the requirement.[33] It is unclear whether 'damage' is limited to pecuniary loss[34] or whether it extends to non-pecuniary loss such as stress and anxiety; there are persuasive arguments that it should so extend.[35] In practice enforcement notices are relatively rare, although they were issued in 2009 to some companies in the

[27] As above, s 51.
[28] As above, s 42.
[29] See generally Rosemary Jay, *Data Protection Law and Practice*, 4th edn, 2012, chapter 20.
[30] A notice to provide the Commissioner's Office with specified information within a specified period to determine whether the data protection principles are being followed: DPA 1998, s 43.
[31] A notice requiring the data controller to take specified steps such as destroying data or refraining from processing specified data , which may be served if the Information Commissioner is satisfied that a data controller has contravened any of the data protection principles: DPA 1998, s 40.
[32] These may be issued if there has been a 'serious' contravention of any of the data protection principles of a kind likely to cause substantial damage or substantial distress and either the data controller knew or ought to have known that there was a risk of a contravention of this nature which it failed to take reasonable steps to prevent or the contravention was deliberate: DPA 1998, s 55A. There is a right of appeal against the decision to issue an information, enforcement or monetary penalty notice.
[33] DPA 1998, s 13.
[34] *Johnson* v *MDU* [2007] EWCA Civ 262, (2007) 96 BMLR 99.
[35] *Murray* v *Express Nwespapers Ltd* [2008] EWCA Civ 446, [2009] Ch 481, [63]; see also *Vidal-Hall and others* v *Google Inc*, above, note 12, at [83]-[103] which refers to the Reasoned Opinion to the UK issued by the European Commission which requested the UK to apply the right to compensation for 'moral damage' when personal information is used inappropriately (press release 24 June 2010) .

construction industry which had purchased information on workers whose trade union activity and other details appeared on a 'blacklist' of workers compiled by an organisation called the 'Consulting Association'.[36] Litigation is currently being pursued by their union on behalf of individuals known to have been affected by this 'blacklisting', which includes a claim for damages under the DPA 1998. I have been unable to find any other reported cases of individuals suing for damages under the Act in the employment context.

Legislation on the interception of communications

2.10 The *Regulation of Investigatory Powers Act* ('RIPA) 2000 regulates the interception of communications and was designed to implement the EC Telecommunications Data Protection Directive.[37] The Directive (now succeeded by the Privacy and Electronic Communications Directive[38]) requires the confidentiality of electronic communications to be respected but allows for certain derogations, of which interceptions for business purposes is one. Like the DPA, RIPA covers employers but also applies beyond the employment context.

2.11 RIPA permits the sender or recipient of a communication on a private telecommunications network to seek an injunction against, or damages for any loss incurred from, an employer who intercepted a communication to or from its own system if the interception was without 'lawful authority'.[39] RIPA specifies a range of circumstances where 'lawful authority' is deemed to exist. Those most relevant to employment are set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,[40] which allow interception of communications on the system used for the purposes of a business by, or on behalf of, the person carrying on the business where specified conditions are met. These Regulations are discussed in greater detail in paragraph 5.4 below.

Access to medical reports

2.12 The *Access to Medical Reports Act* ('AMRA') 1988 gives individuals a right of access to reports on their health (physical or mental) by a medical practitioner responsible for their clinical care which are to be supplied for employment or insurance purposes.[41] Individuals are entitled to see a report before it is supplied and to request amendments to any part which they consider incorrect or misleading. The medical practitioner may refuse to make the amendments but must, if the individual so requests, attach a statement of the individual's views to the report.[42] An employer or prospective employer who proposes to apply for a report must notify the worker in advance of this and must inform him or her of

[36] See K Ewing, *Ruined Lives: Blacklisting in the UK Construction Industry*, Institute of Employment Rights, 2009. In 2010 legislation was introduced specifically prohibiting blacklisting: see Deakin and Morris, above, note 17, paras 8.27-8.32.
[37] EC Directive 97/66 EC.
[38] Directive 2002/58/EC.
[39] RIPA 2000, s. 1(3). 'Private telecommunications system' and 'interception' are defined in s. 2.
[40] SI 2000 No 2699.
[41] AMRA 1988, s 1, 2. Note that the restriction to a practitioner 'responsible for their clinical care' may exclude the employer's occupational health doctor: see further para 4.4 below.
[42] As above, ss 4,5. There are certain exemptions to the right of access, including where the practitioner considers that disclosure would be likely to cause serious harm to the physical or mental health of the individual or others or would indicate the intentions of the practitioner in respect of the individual: s 7. The report cannot then be supplied to the employer unless the individual explicitly consents to this.

the right to withhold consent; of the rights relating to access to the report and its amendment; and of the right, once given access, to withhold consent to the report being supplied.[43] Individuals who consider that their rights under the Act have been, or are likely to be, breached can apply to the courts which can order compliance with the Act.[44] Rights under AMRA need to be considered in the context of other restrictions on medical reports discussed in paragraphs 4.3 and 4.4 below.

Information about criminal offences

2.13 The Rehabilitation of Offenders Act ('ROA') 1974 provides that after periods ranging between two and 11 years, depending on the sentence, criminal convictions become 'spent', although prison sentences exceeding 48 months are excluded.[45] ROA applies in the employment context although it also applies more widely. For the purposes of employment, an individual is entitled to conceal a 'spent' conviction in answer to a question from a prospective employer and 'the person questioned shall not be subjected to any liability or otherwise prejudiced in law by reason of any failure to acknowledge or disclose a spent conviction or any circumstances ancillary to a spent conviction'.[46] In this context, therefore, an individual may give false information without this giving rise to the normal legal consequences of misrepresentation. There are numerous exemptions to the right to conceal a 'spent' conviction in relation to posts in the criminal justice system and other areas of public employment, the professions, and other occupations involving trust and confidence such as those in the medical and financial service sectors.[47]

Equality legislation

2.14 The Equality Act ('EqA) 2010 makes it unlawful to discriminate against an individual because of a 'protected characteristic' in the area of employment[48] and in several other fields, including the provision of goods and services. The protected characteristics are age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; and sexual orientation.[49] Although (pre-employment health inquiries apart)[50] it is not unlawful under EqA to obtain information relating to protected characteristics it is unlawful to use such information to discriminate against individuals and a number of these characteristics[51] constitute 'sensitive personal data' under the DPA 1998. Individual equality rights in the employment field are enforced by complaining to an employment tribunal which may award a declaration of rights; financial compensation to put the claimant in the position he or she would have been in had the discrimination not occurred, including injury to feelings; and a

[43] As above, s 4.
[44] As above, s 3.
[45] ROA 1974, s 5.
[46] ROA 1974 ,s 4(2)(b).
[47] Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, SI 1975/1023.
[48] The legislation covers persons employed under a contract of employment, apprenticeship or a contract 'personally to do work': EqA 2010, s 83(2).
[49] EqA 2010, s 4.
[50] See para 4.3 below.
[51] The racial or ethnic origin of the data subject; religious beliefs or other beliefs of a similar nature; and his or her physical or mental health or condition or sexual life.

recommendation that the respondent takes steps to obviate or reduce the adverse effect of the matter to which the proceedings relate on the complainant or any other person.[52]

Common law

2.15 Misuse of employees' personal information may give rise to actions for breach of confidence; or (possibly) the tort of misuse of private information (see paragraph 2.5 above).[53] Recent proceedings of this kind have focussed on alleged intrusions into the private lives of 'celebrities' by the media rather than by employers and although in theory workers could seek an injunction or damages from the courts, in practice the expense of doing this, and complexity of the law, makes this an unlikely option. Where there is a subsisting employment relationship a failure to protect an employee's personal information would almost certainly breach the contract of employment, and it is strongly arguable that any conduct by an employer that breached the employee's rights under Article 8 of the ECHR would breach the implied contractual duty of trust and confidence.[54]

3. Obtaining Information and Monitoring Employees: Legitimate Purposes

3.1 With a few exceptions (such as tax and social security law) English law does not identify the particular purposes for which it is proper and reasonable for employers to obtain employees' personal information. Rather determining what is proper and reasonable is decided by applying general criteria to particular situations. This section starts by outlining those general criteria and then gives some examples of how they may apply in given situations. It should be noted that, with specific exceptions, the law does not directly prohibit employers *seeking* to obtain information to which they may not be entitled, a considerable gap in protection.

3.2 All the English legislation directly regulating the provision of employees' personal information and monitoring of employees envisages circumstances where an employer's legitimate business interests may allow information to be obtained even if the employee does not consent to this. Under the DPA 1998 the tests of whether personal data is processed 'fairly and lawfully' include the processing being 'necessary' for one of the following:

(1) the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;

(2) compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract; and

(3) 'the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.'[55]

[52] EqA 2010, s. 124.

[53] See *Campbell* v *MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *OBG Ltd* v *Allen and Douglas v Hello!* [2008] 1 AC 1 and other cases cited in *Vidal-Hall,* above, note 12.

[54] This would entitle the employee to claim damages and, probably, to terminate the contract without notice.For discussion of this complex area see Deakin and Morris, above, note 17, chapter 5.

[55] DPA 1998, Sched 1, para 1; Sched 2.

The first two of these tests are very specific. An example of (1) would be obtaining a worker's bank account details for payment purposes; an example of (2) obtaining the worker's tax and social security references so that appropriate statutory deductions from pay could be made. The third is much more open-ended and, according to the UK Supreme Court (UKSC) in *South Lanarkshire Council* v *The Scottish Information Commissioner*, requires three questions to be addressed:

> (a) is the employer pursuing a legitimate interest or interests?
> (b) is the processing involved necessary for the purposes of those interests?
> (c) is the processing unwarranted in this case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject?[56]

In the case of 'sensitive personal data' one of a number of additional tests must also be satisfied. Other than 'explicit consent' those most likely to apply in the context of employment are that:

> (1) the processing 'is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment' and
> (2) the information 'has been made public as a result of steps deliberately taken by the data subject'.

A further test allows monitoring of information relating to racial or ethnic origin in order to promote equality of opportunity.[57]

3.3 In *South Lanarkshire Council* the UKSC held, following the decision of the European Court of Justice in *Rechnungshof* v Ö*sterreighischer Rundfunk* (the *Austrian Radio* case),[58] that if data processing involves an interference with the data subject's right to respect for private life under Article 8(1) of the ECHR then, to be lawful under the DPA 1998, Article 8(2) must be satisfied. Article 8(2) requires the restriction to be 'in accordance with the law'; to pursue a legitimate aim; and to be 'necessary in a democratic society'. 'In accordance with the law' requires the restriction not only to have a basis in domestic law but also to be adequately accessible and formulated with sufficient precision to enable the individual to regulate his conduct and to be able to foresee, to a degree that is reasonable in the circumstances, the consequences which a given course of action may entail'.[59] In the employment context these criteria suggest that any restrictions on private life should be clearly specified in writing and that this document should be made available to all those to whom the restrictions apply. 'Legitimate aims' under Article 8 include 'protection of the rights and freedoms of others'; protection of the employer's property interests against theft[60] and the safety of fellow workers and passengers[61] have been regarded by the ECtHR as legitimate aims. For an interference with the right to be 'necessary in a democratic society' there must be a 'pressing social need' for it; the interference must be 'proportionate to the legitimate aim pursued' and the reasons for it must be 'relevant and sufficient'.[62]

---

[56] *South Lanarkshire Council* v *The Scottish Information Commissioner* [2013] UKSC 55; [2013] IRLR 899, Lady Hale at [18].
[57] DPA 1998, Sched 1, para 1; Sched 3.
[58] Case 465/00, C-138/01, C-139/01 [2003] ECR 1-4989.
[59] *Sunday Times* v *UK* judgment of 26 April 1979, (1979-80) 2 EHRR 245, para 49.
[60] *Köpke* v *Germany* decision of 5 October 2010, [2010] ECHR 1725.
[61] *Madsen* v *Denmark*, App 58341/00, 7 November 2002.
[62] *Handyside* v *UK* judgment of 12 December 1976, (1979-80) 1 EHRR 737, paras 48-50.

3.4 It is possible that data processing may not involve an interference with an individual's private life. This may be on the basis that the individual has already placed the information in the public domain (it is hard to see that obtaining information from an individual's open-access web-site would intrude on privacy, for example),[63] or if the court adopts the view that the employer has shaped the scope of 'private life' by contract or a warning (see paragraph 2.3 above). Even then, however, the UK courts have emphasised that the requirement in the DPA 1998 for the processing of any personal data (consent aside) to be 'necessary' for a specified purpose means that it must serve a 'pressing social need' and be 'both proportionate as to means and fairly balanced as to ends'.[64]

3.5 Beyond these general principles there is very little 'hard law' as to the purposes for which employers may properly and reasonably obtain information and how these purposes are to be balanced with employees' privacy protection. The Information Commissioner's Employment Practices Data Protection Code ('EPDPC'), referred to in paragraph 2.8 above, considers in detail how employers should decide what information they need at particular stages of the employment relationship and emphasises that they should always ask themselves why they require it and whether they are asking for more information than they really need . However, whilst it provides very useful guidance, this Code has no legal status. The paragraphs that follow are, therefore, based on the application of the general principles outlined in paragraphs 3.2 - 3.4 above, with examples taken from the EPDPC, and the 'Supplementary Guidance' ('SG') to it, where appropriate .

3.6 Looking first at recruitment, this will necessarily involve an employer collecting a basic level of information about all applicants, such as their contact details, qualifications and previous experience. It is hard to see how this could prejudice applicants' legitimate interests. However the collection of more detailed information, such as identity checks, may be appropriate only in relation to short-listed candidates and more intrusive forms of pre-employment vetting appropriate (if at all) only in relation to a candidate it is intended, subject to satisfactory vetting, to appoint. Specific restrictions on personal information in the hiring process are dealt with in section 4 below.

3.7 Once employment starts, employers will need to keep records of employees' attendance/absence from work in order to calculate pay and allowances. However the EPDPC/SG recommends that, work-related injuries aside,[65] employers should either avoid keeping records of employees' specific illnesses or injuries, which constitute 'sensitive personal data', or, if such records are needed to monitor the ability of an individual to work or to detect hazards at work, should at least segregate them from absence data. Keeping records for disciplinary purposes is also legitimate and indeed, employers are advised to keep such records[66] although disciplinary procedures should specify whether a disciplinary sanction, such as a warning, that has expired should be removed from the record. Where an undertaking is being transferred there is now a statutory obligation on the transferor to supply 'employee liability information' to the transferee which identifies the employees to

[63] See also DPA 1998, Sched 3, para 5.

[64] *Corporate Officer of the House of Commons* v *Information Commissioner* [2008] EWHC 1084, [1009] 3 All ER 403, cited with approval in *South Lanarkshire Council* v *The Scottish Information Commissioner*, above, note 56, at [19]; see also [27].

[65] Employers are advised to maintain an 'accident book' as part of their health and safety policy and there is a statutory duty to report some injuries and diseases: see Reporting of Injuries, Diseases and Dangerous Occurances Regulations 2013 SI 2013 No 1471.

[66] See Acas Code of Practice *Disciplinary and Grievance Procedures* (2009), foreward; *Acas Guide: Discipline and Grievances at Work* (2009).

be transferred and includes specified information about them including their age and any disciplinary procedure against them.[67] This is exempt from the non-disclosure provisions of the DPA 1998[68] but other obligations relating to personal data will need to be observed.

3.8 It is generally recognised that employers have a legitimate interest in monitoring their employees' performance at work, including the output and quality of their work and whether they are following safe working practices. However the method by which this is done should be proportionate and not unnecessarily intrusive. The EPDPC suggests that employers should conduct an 'impact assessment' which involves looking at the purposes behind monitoring and the benefits it is likely to deliver; identifying any likely adverse impact; considering the alternatives to monitoring; and then judging whether monitoring is justified. The EPDPC emphasises the importance of ensuring that workers are aware that monitoring is taking place and why, unless exceptional circumstances justify covert surveillance (see paragraph 5.9 below). The protection of the employer's trade secrets and other property interests would be a proper reason for monitoring but probably only on a targeted basis following specific intelligence that such property is at risk from a particular worker or group of workers. Specific issues relating to video surveillance and the monitoring of electronic communications are dealt with in paragraphs 5.3-5.7 below.

4. Personal Information Protection in the Hiring Process

4.1 Job applicants are particularly badly protected in English law. The only areas where employers are specifically restricted in asking for information relate to health and criminal records and even then the restrictions are fairly narrow.

Criminal proceedings

4.2 Under the *Rehabilitation of Offenders Act* ('ROA') 1974, described in para 2.13 above, (excepted employments apart) an individual is entitled to conceal a 'spent' conviction without being subject to any liability for non-disclosure.[69] The ROA itself does not make it unlawful for the employer to *seek* to obtain this information but obtaining it could breach the principle in the DPA 1998 that data should be processed 'fairly and lawfully' and support a claim for damages if the applicant was denied a job as a result.[70] Moreover, it is a criminal offence under the DPA for an employer "in connection with" the recruitment of a person as an employee, or their continued employment, to require that person (or a third party) to supply the employer with specified information obtained under the right of access to data described in paragraph 5.11 below.[71] The information covered by this ban on enforced subject access relates, broadly speaking, to criminal records and

[67] Transfer of Undertakings (Protection of Employment) Regulations 2006, SI 2006 No 246, reg 11, as amended. Where due diligence exercises outside these provisions are being undertaken, or information is sought beyond the scope of TUPE reg 11, the Information Commissioner recommends that wherever possible information about workers should be anonymised.
[68] DPA 1998, s 35.
[69] ROA 1974, s 4(2)(b).
[70] DPA 1998, s 13.
[71] DPA 1998, s 56. See Jay, above, note 29, chapter 27 for discussion of this provision, which was introduced to prevent what the then Data Protection Registrar saw as a growing practice of individuals being required by employers to use their right of access to obtain a copy of their criminal record from the police. The EPDPC goes beyond the Act in stating that applicants should not be forced to use their subject access rights to obtain *any* records from another organisation (para 1.3.1).

national insurance records which can reveal if time has been spent in custody or gaps in employment (although at the time of writing only part of this provision has been brought into force).[72] Of more general current relevance, the commission or alleged commission of a criminal offence or any proceedings for any offence committed by an individual; the disposal of such proceedings; or the sentence of the court constitute 'sensitive personal data' under the DPA; these matters are therefore subject to the tighter controls relating to the processing of such data set out in paragraph 3.2 above. The EPDPC states that employers should seek information about an applicant's criminal convictions only to the extent that this has a direct bearing on his or her suitability for the job in question.

Health and medical information:

4.3 The *Equality Act* ('EqA') 2010 makes it unlawful for a person (A) to 'whom an application for work is made' to 'ask about the health of the applicant (B)' either 'before offering the work to B' or, where A is not in a position to offer the work, 'before including B in a pool of applicants from whom A intends (when in a position to do so) to select a person to whom to offer work'.[73] Whether or not a person has a disability is an aspect of that person's health,[74] and the provision is designed to ensure that disabled applicants are assessed objectively for their ability to do the job in question.[75] However the protection it offers is qualified. First, the fact that an employer has asked an applicant about his or her health does not give the applicant an automatic right of action, although if the applicant takes a case to an employment tribunal and contends that the employer's conduct in reliance on information given in response to such a question amounts to direct discrimination the employer will then bear the burden of proving that it did not discriminate.[76] Second, there are a number of situations in which employers can continue to make pre-employment health checks under EqA 2010. These include where the purpose of the question is to establish whether B 'will be able to comply with a requirement to undergo an assessment' or in establishing whether A will need to make reasonable adjustments in connection with such a requirement; in establishing whether 'B will be able to carry out a function that is intrinsic to the work concerned' once reasonable adjustments have been made; and in monitoring diversity in the range of persons applying to A for work.[77]

4.4 A person's 'physical or mental health or condition' constitutes 'sensitive personal data' under the DPA 1998 so the employer would need to satisfy the tests discussed in paragraph 3.2 above to obtain such information. The inclusion of 'condition' as well as health seems wide enough to include pregnancy; whether biometric data, particularly genetic data, is covered is unclear.[78] The *Access to Medical Reports Act* ('AMRA') 1988, outlined in paragraph 2.12 above, will also need to be complied with if the employer seeks

[72] The provision relating to those barred from working with children and vulnerable adults is now governed by a specific regime (see para 4.7 below). As Jay explains, the aim is that, where appropriate, employers have legitimate access to information under a regulated channel.
[73] EqA 2010, s 60(1).
[74] Above, s 60(13).
[75] Equality and Human Rights Commission, *Code of Practice on Employment* (2011), para 10.27.
[76] Above, s 60(3)-(5). The prohibition on asking questions can be enforced directly by the Equality and Human Rights Commission: s 60(2), 120(8).
[77] Above, s 60(6),(7).
[78] The draft EU General Data Protection Regulation, art 9, specifically refers to 'genetic data': COM (2012) 11 final.

a medical report at the hiring stage, although as it is limited to reports provided by a medical practitioner 'who is or has been responsible for the … [applicant's] … clinical care' it would probably not apply to a report by the employer's occupational health service with which the applicant had no prior relationship. A weakness of both the DPA and AMRA is that there is no protection against discrimination in either Act for an applicant on the ground that they have refused to comply with an employer's request for a report or other data.

Information on other matters

4.5 English law does not specifically prevent an employer *requesting* information about matters beyond those discussed above, although the DPA 1998 applies to *obtaining* and otherwise processing personal data or 'sensitive personal data'. In particular there are no restrictions like those in ROA 1974 relating to a candidate's civil litigation history, including employment litigation, although it may be a breach of the Equality Act 2010 not to hire someone because they have previously brought proceedings under that Act.[79] Civil litigation history (unlike criminal proceedings) does not constitute 'sensitive personal data' for the purposes of the DPA 1998. Employers can obtain an individual's 'public credit record' which includes electoral roll information (including address), insolvency records, county court judgments and any notices of correction. They have no right of access to an individual's credit history beyond this, such as their payment record, but if an employer insisted on a candidate providing such information and the candidate refused there seems nothing to prevent the employer declining to recruit the individual for that reason.

4.6 The fact that an employer sought information about matters that constitute 'protected characteristics' under EqA 2010 (see para 2.14 above) could be used in evidence in a claim of direct discrimination if the employer decided subsequently not to employ the individual, although in practice comparatively few discrimination cases have been brought in connection with recruitment, which raise particular problems of proof.[80] (It would be easier to show discrimination if the employer sought particular information from some applicants and not others, for example selectively asking about religious beliefs on the basis of applicants' race or colour.) Employers who access applicants' social media profiles are likely to learn about many of their characteristics, such as their age, marital status, sexual orientation, and ethnicity. However mounting a successful discrimination claim on the basis of this evidence alone would be extremely difficult. It is unlawful to deny an individual employment on the basis of their union (or non-union) membership (including membership of a specific union).[81] Again inquiring about an applicant's union membership status could constitute evidence of discrimination.[82] Specific measures to prohibit the compilation of 'blacklists' of union members and activitists to which employers can subscribe have recently been introduced following exposure of the

[79] EqA 2010 s 27 states that a person A victimises another person B if A subjects B to a detriment because B does a protected act (or A believes that B has done or may do a protected act), which includes bringing proceedings under EqA 2010 or doing any other thing in connection with it and s 39 makes it unlawful to victimise a person by, among other things, not offering them employment. The point has not been tested in the courts.

[80] Broughton *et al*, above, note 2, p 10.

[81] See generally Deakin and Morris, above note 17, paras 8.21-8.37 for detailed discussion of this area.

[82] This also constitutes 'sensitive personal data' under the DPA 1998, s.2.

widespread use of such blacklists in the construction industry.[83] Although 'religion or belief' are 'protected characteristics' under EqA 2010 there is no express protection at the hiring stage against discrimination on the basis of political views.[84] The English courts have held that political opinions which are capable of amounting to a 'philosophical belief' fall within the term 'belief' but not membership of a political party *per se*.[85] An individual's 'political opinions' are 'sensitive personal data' under the DPA 1998.

4.7 English law does not in general specify in positive terms the information that an employer is entitled to obtain regarding its employees, although all employers are required to check that workers have the legal right to work in the UK which involves scrutiny of official documentation such as passports or residence or work permits.[86] However there are particular provisions which govern particular occupations: candidates for appointment as police officers, for example, can be required to undertake tests for substance misuse.[87] A government 'Disclosure and Barring Service' is designed to prevent people from being recruited to work with vulnerable groups by processing requests for criminal record checks and placing people on children's and adults' 'barred lists' which employers must check before recruiting staff.

5. Personal Information and Privacy Protection during the Employment Relationship

5.1 The general principles which govern the purposes for which employers are entitled to obtain employees' personal information have been outlined in section 3 above. In addition, once the employment relationship has started the contractual terms that govern it may be significant in demonstrating the worker's 'consent' or 'explicit consent' to the employer obtaining and holding information.[88] The only direct restriction on contract terms in this area[89] is contained in the DPA 1998 which makes void any contractual requirement that an individual should use their right of subject access to supply a 'health record', defined as any record consisting of 'information relating to the physical or mental health or condition of an individual" made "by or on behalf of a health professional in connection with the care of that individual".[90] This definition is wide enough to cover a record compiled by a previous employer's occupational health adviser as well as by the worker's own physician.

[83] Employment Relations Act 1999 (Blacklists) Regulations 2010, SI 2010/493. See para 2.9 above and Deakin and Morris, above, note 17, paras 8.27-8.32.
[84] In 2013 the UK Government removed the requirement of a qualifying period of employment to bring an unfair dismissal claim where the dismissal relates to the employee's 'political opinions or affiliation' (Employment Rights Act 1996, s 108, as amended) in response to the ECtHR decision in *Redfearn* v *UK* judgment of 6 November 2012, (2012) ECHR 1878 that there was a breach of Article 11 of the ECHR because the applicant had been dismissed because of his membership of the British National Party with no right for the justification for this to be considered by a court or tribunal.
[85] *Grainger* v *Nicolson* [2010] IRLR 4, EAT; *Baggs* v *Fudge* ET/1400114/05.
[86] See generally Home Office, *Full guide on preventing illegal working in the UK for employers*, 2013.
[87] The Police Regulations 2003, SI 2003/527.
[88] See further paras 2.3 above and 7.2 below.
[89] See also para 2.5 for the effect of Article 8 of the ECHR under the HRA 1998 on interpretation of the contract.
[90] DPA 1998, ss 57, 68. Employment legislation generally provides that an agreement by an individual to waive protective rights is void: see, for example, Employment Rights Act 1996, s. 203(1).

5.2 Where the employee has not 'consented' to the provision of personal information the principles that will govern whether the employer is entitled to obtain personal information will be those set out in paragraphs 3.2 - 3.4 above. Some examples of the types of information that employers would seem entitled to obtain was given in paragraphs 3.6-3.8. The application of the general principles suggests that employers should not collect information about workers' off-duty conduct unless it has clear implications for their ability to do their job or poses a real risk to the employer (for example in areas of financial services information about a worker's gambling habit may justify investigation). Other examples would be to ascertain whether the worker is working elsewhere, which may have implications for statutory working time limits or the protection of trade secrets. Moreover, the ECtHR has held that the fact that drug or alcohol testing at the commencement of a shift may reveal information about a worker's off-duty conduct will not, of itself, make collecting that information unlawful if it is otherwise justified for safety reasons.[91]

5.3 Video surveillance is a particularly intrusive form of monitoring. There are no legal provisions in English law relating to video surveillance of workers beyond those applicable to monitoring in general. However the Information Commissioner has issued a (non binding) Code on closed-circuit television ('CCTV') which considers that continuous monitoring should be used only in very exceptional circumstances, such as where hazardous substances are used and failure to follow procedures would pose a serious risk to life, and workers should be told it is being deployed. The Code considers that CCTV may also be justified in an area of its premises that a employer considers particularly vulnerable to theft, such as a store room, but not in areas such as toilets or private offices. Where CCTV is being used to prevent and detect crime by customers, such as in shops, it should not be used to monitor the workforce for non-criminal matters such as performance or compliance with company procedures.[92]

5.4 Monitoring of workers' electronic communications, like other forms of monitoring, is subject to the DPA 1998. Where monitoring involves the interception of a communication between a sender and recipient, such as a telephone call or e-mail, the interception will need to be lawful under RIPA 2000, outlined in paragraphs 2.10 and 2.11 above. [93] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations ('LBPR') 2000 made under RIPA allow interceptions to monitor or keep a record of electronic communications relevant to the employer's business for a range of purposes including ascertaining compliance with regulatory or self-regulatory practices or procedures; investigating or detecting unauthorised use of telecommunications systems; and monitoring communications to see if they are of a business nature (the 'routine access' exception). The employer must make 'all reasonable efforts' to inform every person who may use the system that communications may be intercepted but need not obtain their consent.[94] There is no restriction on what employers

[91] *Madsen* v *Denmark* above, note 61.
[92] Information Commissioner, *CCTV Code of Practice*, 2008, App 3.
[93] 'Interception' occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. In *R v Coulson* [2013] EWCA Crim 1026 the Court of Appeal held that 'the course of transmission' may continue even though the message has already been received and read by the intended recipient.
[94] See generally reg 3. Interception is lawful under RIPA 2000 where both the sender and recipient consent to the interception but obtaining the consent of external third parties is likely to be difficult. The need to inform under LPBR could also be difficult where the communication is initiated by an external third party.

may designate as 'unauthorised' use nor does LBPR require them to demonstrate that they have any grounds to suspect unauthorised use prior to instigating interception or that interception is a proportionate response to any problem.

5.5 Concern was expressed that interceptions authorised under LBPR for business purposes could also mean that workers' personal telephone calls and e-mails could be intercepted, which would breach the right to respect for private life unless justified under Article 8(2) of the ECHR.[95] On one view it can be argued that if employers have a clear policy that forbids the use of its communications systems for private purposes, which is enforced in practice to avoid any expectation of privacy, workers take the risk that any personal communications sent or received are at risk of interception under the 'unauthorised use' or 'routine access' provisions.[96] Although at one time such a policy may have been seen as unreasonably restrictive the widespread ownership of mobile and smart phones could be seen as lessening this objection as workers can continue to receive communications when at work. However there is still the risk that workers will receive communications from external parties of a personal nature or communications from those within the organisation such as the occupational health department or a trade union. The Information Commissioner suggests a range of steps that employers can take to reduce the risk of intercepting such communications, such as setting up a system that avoids messages from particular individuals or sections of the organisation being subject to monitoring.[97]

5.6 The fact that data has been obtained lawfully under LBPR does not mean that its processing is lawful under the DPA; processing will need to comply with criteria which, as discussed in paragraphs 3.2-3.4 above, scrutinise much more closely the need for monitoring and whether it is proportionate. In relation to other aspects of internet use, such as web-browsing and use of social media, employers are also recommended to have clear policies on what is acceptable and how these policies will be enforced; in this area the Advisory, Conciliation and Arbitration Service ('Acas') recommends having equivalent standards of behaviour for the 'on-line' and 'off-line' worlds. Acas also recommends developing these policies in consultation with the workforce, an approach which may assist an employer in defending its policies against challenge. The Information Commissioner suggests that, if private internet access is allowed, it could be separated from business access by having a different log-on for private use and then limiting the collection of information on private use to the length and time of the session.[98]

5.7 The distinction between on and off-duty conduct may be particularly difficult to draw in the 'on-line' world where workers may move rapidly between the personal and business realms. Moreover, off-duty activities in the on-line world may affect the workplace. Acas recommends employers' bullying and harassment policies should cover cyber-bullying of other workers regardless of when and where it occurs and that employers should monitor social networking sites if employees report breaches of the policy.

Telephone calls can be preceded by a pre-recorded messages; for e-mails this can be done only after the first communication but the employer who does this would probably be seen as having made 'reasonable efforts'.

[95] *Copland* v *UK* above note 5.

[96] The requirement that interception be 'effected solely for the purpose of monitoring or … keeping a record of communications relevant to the … business' probably means that even unauthorised personal e-mails cannot be the *target*, as opposed to the by-product, of monitoring but the matter is not free from doubt. Monitoring to detect leakage of trade secrets would seem to be lawful.

[97] *EPDPC Supplementary Guidance*, para 3.2.7.

[98] Above.

5.8 Technology enabling workers to work away from the workplace may mean that employers fund workers' electronic equipment, such as a mobile phone or landline, which is used for both personal and business use. The EPDPC emphasises the need for employers to make workers aware of the information they receive as a result of these arrangements (itemised bills, for example) and states that they should not make use of information about private calls 'unless they reveal activity which no employer could reasonably be expected to ignore' such as criminal activity, gross misconduct or practices that jeopardise the safety of others. It takes the same approach to the monitoring of vehicle use by devices which can record or transmit information such as the location, distance travelled, and the individual worker's driving habits. Here the EPDPC suggests the installation of a 'privacy button' or similar arrangement to enable the monitoring to be disabled when the vehicle is being used for private purposes.

5.9 In general, workers should always be informed of surveillance or monitoring. However there are circumstances where 'covert' monitoring or surveillance will be regarded as legitimate.[99] The EPDPC stresses that it should be used only in exceptional circumstances such as where there are grounds for suspecting criminal activity or equivalent malpractice and notifying individuals about the monitoring would prejudice its prevention or detection. However, in assessing whether an employee's dismissal was fair on the basis of evidence obtained through covert monitoring the courts have taken a less restrictive approach than this Code suggests. In a 2004 decision the Employment Appeal Tribunal (EAT) considered that where the employer suspected that the employee, who worked in a water treatment plant and lived nearby, was falsifying time sheets, covert surveillance of his house served a legitimate aim (the protection of company assets); was not disproportionate in the circumstances; and did not breach Article 8 of the ECHR.[100] In a more recent decision the EAT held that covert surveillance showing the claimant at a sports centre during the time when he should have been at work (following initial sightings by a co-employee) either did not constitute an 'interference' with his right to respect for private life, as the claimant was in a 'public place' or, if it did, the employer was pursuing the legitimate aim of protecting its contractual rights.[101] The Employment Tribunal (the first instance decision-maker) in this case had found the employer's decision unfair because the employer had not followed the EPDPC and, indeed, seemed to be ignorant of it. The EAT did not see why 'ignorance of a code which the employer was not bound in law to have regard to in any event would render an investigation into the wrongdoing of the claimant unreasonable when it would otherwise have been reasonable'.[102] This is an example of the lack of integration of English data protection and employment law to which I return in the concluding section of this paper.

5.10 The disclosure of a disciplined employee's name or other work-related information within or outside the employer's organisation has not been a general issue of discussion from a privacy perspective.[103] The advice of Acas is that disciplinary records

[99] See *Kopke* v *Germany*, above, note 60, where the employee's complaint that covert video surveillance by the employer infringed Article 8 of the ECHR was dismissed.
[100] *McGowan* v *Scottish Water* [2005] IRLR 167. The court did not clearly separate the issues arising under Article 8(1) and 8(2).
[101] *City and County of Swansea* v *Gayle* [2013] IRLR 768.
[102] Above at [29].
[103] EqA 2010, s 77 introduced a new provision making unenforceable a contractual term which seeks to prevent a person obtaining disclosure from a colleague about that colleague's pay but that is in the specific context of finding out whether there is unlawful discrimination.

should be kept confidential, and disclosing them without the employee's consent would be a breach of the DPA 1998, assuming that the records constituted 'data' within the meaning of the Act (see paragraph 2.6 above). Disclosure would also be likely to constitute a breach of the implied duty of trust and confidence owed to the employee.[104] However there may be circumstances where disclosure could be seen as justified. In *Rechnungshof* v Ö*sterreighischer Rundfunk*[105] the ECJ stated that disclosing data about the pay of those working for certain public bodies had the legitimate aim of the economic well-being of the country (exerting pressure on those bodies to keep salaries within reasonable limits) and was 'necessary in a democratic society' to achieve that aim. The British Home Secretary has recently announced the intention of compiling a national register of dismissed police officers with the aim of preventing them from being recruited by other local police forces.[106]

5.11 Workers' rights of access to personal information held by their employer is governed by the general principles regulating all 'subject access' contained in the DPA 1998. On receipt of a request in writing and a maximum £10 fee employers must supply workers with the information, including information as to its source, within 40 days of the request. The information must be communicated to the worker 'in an intelligible form' with an explanation of any non-intelligible terms (codes, for example).[107] In addition, where an employer processes the worker's personal data by automatic means to evaluate matters such as work performance, conduct and reliability, and that processing is likely to constitute the sole basis for any decision significantly affecting him or her, the worker is entitled to be informed of the logic of that decision-taking.[108] An individual may give written notice to the employer to cease processing any personal data on the ground that the processing is causing or is likely to cause substantial and unwarranted damage or distress to him or her, or another, which may be enforced by court order but there are certain exceptions to this right, including the worker having consented to the processing and the processing being necessary to the performance of the worker's contract or compliance with an employer's legal obligation.[109] An employer may be ordered by a court to correct, erase or destroy inaccurate personal data;[110] in practice, it is to be hoped that this could be done in the employment context by agreement between the parties. It is strongly arguable that failure by an employer to correct inaccurate data would constitute a breach of the implied contractual term of trust and confidence.[111]

6. Personal Information and Privacy Protection after the Employment Relation Ends

6.1 The general legal principles concerning personal information and privacy protection continue to apply once the employment relationship ends. In accordance with

[104] See generally Deakin and Morris *Labour Law*, above, note 17, paras 4.105-4.107.
[105] Above, note 58.
[106] Speech by the Home Secretary on police integrity, 12 February 2013.
[107] DPA 1998, ss7, 8. There are certain exceptions to the right of access: see s. 37; Sched 7. There are specific provisions relating to access to information which identifies third parties, including identifying them as a source: s7(4)-(6); see further para 6.2 below.
[108] DPA 1998, s 7(1)(d). See s 12 for rights in relation to automated decision-taking.
[109] Above, s 10.
[110] Above, s 14.
[111] See note 104 above.

the data protection principles in the DPA 1998 former employers should not keep personal data about individuals for longer than necessary.

6.2 A prospective employer will commonly wish to obtain a reference from an applicant's former or current employer and applicants will generally be asked to consent to the disclosure of their personal information for that purpose. References given by the 'data controller' in confidence for the purposes of the employment or prospective employment of the data subject are exempt from the right of subject access described in paragraph 5.11 above.[112] However an individual may be able to obtain a copy of the reference if this is part of the personal data held by the new employer as the exception for references applies only to references 'given by' the data controller. In the case of a information (including a reference) which identifies a specific individual as the source, either the source must consent to the disclosure or it must be 'reasonable in all the circumstances to comply with the request' for disclosure; factors relevant here include any steps taken by the employer to seek consent and whether the source has expressly refused consent.[113] The Information Commissioner considers that references should be released unless the referee provides a 'compelling reason' why they should be edited or not released[114] and it is not uncommon for those seeking references to warn the referee in advance that their reference may be disclosed to its subject.

7. Conclusion

7.1 This paper has sought to explain the broad principles that govern the protection of employees' personal information and privacy in English law. Much of the legislation is technically very complex and its fragmented nature adds to its obscurity. The Code and Supplementary Guidance relating to employment issued by the Information Commissioner is helpful but it has no legal status and cannot, therefore, be relied upon as authoritative (and, indeed, one court has said that it should be completely disregarded: see paragraph 5.9 above). There is now a strong argument for the rights of workers and prospective workers in this area to be the subject of specific legislation which takes full account of, and is integrated into, employment law.[115]

7.2 Important substantive weaknesses in the current law which need correcting include the following:

(a) Ambiguity as to what constitutes 'consent', which is often key to assessing whether employers have lawfully obtained and retained employees' personal data. Under Directive 95/46/EC 'consent' means 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' and Member States must provide that data may be processed only if the data subject has 'unambiguously' given consent.[116] The DPA 1998 does not define 'consent' and the European Commission has found that Member States have interpreted 'consent' differently, ranging from a general requirement of written consent to the acceptance of

[112] DPA 1998, s 37; Sched 7, para 1.
[113] Above, s 7(4)-(6).
[114] *EPDPC Supplementary Guidance*.
[115] For the argument for greater integration at international level see Hendrickx and Van Bever, above, note 7. The ILO Code of Practice on Protection of Personal Data, 1997, offers a good starting-point for considering what such legislation should contain.
[116] Arts 2(h), 7(a).

implicit consent.[117] For 'sensitive personal data' the Directive and the DPA require 'explicit' consent'.[118] This suggests that something additional to what is required for 'bare' consent is needed but it is not clear what this might be.

(b) The absence of protection against discrimination for those who do not 'consent'.[119] At present an individual who refuses to provide personal information, or who challenges the employer's right to seek it and is subsequently prejudiced in employment on that ground, has no statutory protection, nor do individuals who enforce their statutory rights under the DPA 1998 or AMRA 1988.[120] If in employment, it may be possible to argue that an employer's demand for information that breached an employee's rights under Article 8 would breach the implied term of trust and confidence enabling the employee to claim that he or she had been constructively dismissed. However to pursue such a claim in the employment tribunal requires a minimum period of employment (one or two years, depending on when the employment started).[121] The protection for job applicants is even more limited and in today's employment market it is an insufficient response to say that they can always choose to work elsewhere.

(c) There is no general prohibition on an employer *seeking* information which exceeds permitted purposes nor a general protection, like that in ROA 1974, for giving inaccurate or evasive answers if such information is sought (see paragraph 2.13 above).

(d) The remedies for workers are inadequate. The right to damages under the DPA 1998 requires an individual to show that they have suffered 'damage' *by reason of* the employer having contravened the Act, which may not be easy.[122] Those who wish to object to privacy invasions in advance have no right of action and the Information Commissioner's enforcement remedies have not, to date, been widely used. Remedies as well as substantive rights which are specific to employment law are needed.

(e) Workers should have a right to access without charge and to amend (or attach comments to) the personal information which their employers hold regardless of whether that information constitutes 'data' as defined in the DPA 1998 (see paragraph 2.6 above). The general principles governing personal information and privacy should also apply irrespective of the form in which information is collected and stored.

At present there is no indication that the British Government intends to change the law in this area beyond the discussions that are taking place at EU level about changes to wider data protection law.

[117] Commission Communication COM (2010) 609 final of 4 November 2010, para 2.1.5.

[118] Directive 95/46/EC, art 8(2)(a); DPA 1998, s 4(3); Sched 3, para 1.

[119] Cf the conclusions of the Article 29 Data Protection Working Party that consent is not valid if there is a 'real or potential relevant prejudice that arises from not consenting': Opinion 15/2011 on the definition of consent, p 13. The draft General Data Protection Regulation COM (2012) 11 final art 7(4) provides that consent should not provide a legal basis for data processing where there is a 'significant imbalance' between the position of the data subject and the controller.

[120] Cf the protection against victimisation for bringing proceedings or alleging contravention of the Equality Act 2010: EqA 2010, s. 27.

[121] Employment Rights Act 1996, s 108(1), as amended. Where the employee's period of continuous employment began before 6 April 2012 the period is one year.

[122] The Information Commissioner gives as an example a former worker losing a new job offer owing to a reference from the ex-employer which is based on inaccurate data.