

INDUSTRIAL LAW SOCIETY
ANNUAL CONFERENCE 2010 – ST. CATHERINE’S COLLEGE, OXFORD

**BIG BROTHER AND EMPLOYMENT: SURVEILLANCE IN THE WORKPLACE AND
OTHER HUMAN RIGHTS ISSUES**

INTRODUCTION

1. This session considers the right to privacy and its interaction with the employment relationship. It will attempt to give an overview of the current legal framework in this area and show that it is overly complex and unsatisfactory to meet the challenges of the modern workplace.

2. There are inevitable difficulties in seeking to regulate employers’ attitudes towards privacy at work. Employment is the aspect of everyday life most likely to involve necessary (or voluntary) sacrifices of personal privacy, but it is also the arena in which privacy can be most at risk of intrusion. While recent technological advances have facilitated and encouraged larger-scale voluntary sharing of personal information than has ever taken place before (e.g. through social networking websites), they have also made it increasingly cheap and easy for employers to monitor and record private communications and activities.

3. Public attitudes towards privacy have been in a state of flux over the past two decades. Through the 1990s and early 2000s, partly as a result of high profile criminal cases such as that of Jamie Bulger’s killers (who had been captured on CCTV) and Ian Huntley (who had previously come to the attention of the police as a potential threat to children), it became widely accepted that public safety concerns justified a relatively high level of privacy intrusion, for example through increased use of CCTV or employment vetting checks. Following 9/11 the balance shifted still further towards security and away from privacy rights.

4. Liberty produced a report in 2007 entitled *Overlooked: Surveillance and personal privacy in modern Britain*¹. The title had a deliberate double meaning: it referred to the fact that as a society we are now quite literally looked at by hundreds of thousands of cameras; but also that privacy was an overlooked, neglected right. It is not difficult to see why it might have attracted less attention and concern than, e.g., the prohibition on torture or the right to liberty.
5. More recently, however, mass data gathering and surveillance of all types have been met with far greater scepticism by the public, not least because of serious security lapses by a number of government bodies and some high profile examples of misuse of power. There have also been a number of recent legal and political developments which suggest that the tide has now turned:
- The European Court of Human Rights found violations of the right to privacy arising from the blanket retention of DNA profiles on a national database² and stop and search without suspicion under s.44 of the Terrorism Act 2000³.
 - The Court of Appeal recognised that photography in public places may in certain circumstances engage privacy rights.⁴
 - In one of the first judgments to be handed down by the Supreme Court it was held that the regime for Enhanced Criminal Record Checks took insufficient account of privacy rights and needed rebalancing.⁵
 - The Labour government's proposals on ID cards have been scrapped and the "Contactpoint" database holding information on all children in the country has been switched off.
 - The Investigatory Powers Tribunal ruled unlawful a local authority's covert surveillance of a family to enforce its school admission policies.⁶
 - In the last few months, a public outcry at a new counter-terrorism surveillance scheme in two predominantly Muslim areas of Birmingham resulted in the removal of 72 covert cameras and overt cameras being covered with bags pending public consultation.

¹ <http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf>

² *S & Marper v UK* (2009) 48 EHRR 50

³ *Gillan & Quinton v UK* (2010) 50 EHRR 45

⁴ *R (Wood) v Metropolitan Police* [2009] EWCA Civ 414

⁵ *R (L) v Metropolitan Police* [2010] 1 AC 410

⁶ *Paton v Poole Borough Council* (2010, IPT)

6. An enforceable right to privacy under the Human Rights Act 1998 (“HRA”) is a new and welcome feature of the law in the UK, but it currently only applies to public authorities. And the Regulation of Investigatory Powers Act 2000 (“RIPA”), introduced alongside the HRA purportedly to achieve compliance with privacy rights, provides no meaningful protection for workers. Since there now appears to be far greater understanding that a reasonable degree of privacy is fundamental to a free and democratic society, the absence of proper legal protections in the workplace is anomalous and, given the speed of technological advancement, should be addressed urgently.

OVERVIEW OF THE LEGISLATIVE FRAMEWORK

7. Article 8 of the European Convention on Human Rights provides:

Right to respect for private and family life

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.
8. The HRA incorporated Article 8 into UK law by a variety of legal mechanisms, the most significant of which is the obligation in section 6 on public authorities to act compatibly with Convention rights:

Acts of public authorities

- (1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right.
- (2) Subsection (1) does not apply to an act if—
 - (a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or
 - (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions.

- (3) In this section “public authority” includes—
 - (a) a court or tribunal, and
 - (b) any person certain of whose functions are functions of a public nature,
- (4) but does not include either House of Parliament or a person exercising functions in connection with proceedings in Parliament.
- (5) In subsection (3) “Parliament” does not include the House of Lords in its judicial capacity.
- (6) In relation to a particular act, a person is not a public authority by virtue only of subsection (3)(b) if the nature of the act is private.
- (7) “An act” includes a failure to act but does not include a failure to—
 - (a) introduce in, or lay before, Parliament a proposal for legislation; or
 - (b) make any primary legislation or remedial order.

The inclusion of courts and tribunals in the definition of public authorities enables litigants in private litigation to rely on Convention rights in certain circumstances.

9. The HRA was brought into force on 2 October 2000. The state’s obligations under Article 8 are met in part by two further Acts of Parliament which came into force on the same date:
 - Data Protection Act 1998 (“DPA”): implements the Data Protection Directive (1995) and provides additional rights for individuals against “data controllers” as well as a legal basis for certain types of data processing which might otherwise be unlawful under Article 8.
 - Regulation of Investigatory Powers Act 2000 (“RIPA”): provides a mechanism for the authorisation of surveillance powers. Of most relevance to the employment context:
 - Part I forbids interception of communications but provides for exemptions, including specifically in the employment context through the Lawful Business Practice Regulations.
 - Part II provides a legal framework for covert surveillance by public bodies in certain situations and serves as a defence to any civil or human rights claims which might otherwise have been available.

MEANING AND SCOPE OF PRIVACY IN THE WORKPLACE

10. Privacy is a subjective and wide-ranging concept that does not lend itself to simple definition (although many have tried). It may be useful instead to identify some of the principal aspects of privacy that may be at issue in the workplace:

- Informational privacy: collection, use, tracking, retention and disclosure of personal information
- Physical privacy: protection of the body from outside interference
- Spatial privacy: protection of personal spaces, such as the home and (in some circumstances) the workplace
- Relational privacy: freedom to determine one's associations with others, including by private correspondence

11. Although the scope of privacy rights is inevitably restricted in working environments, in large part due to the realities of people management and employers' legitimate interests in protecting their property, a general obligation to respect workers' privacy is now well-established in the case-law of the European Court.

12. In *Niemietz v Germany* (1993) 16 EHRR 97 the Court defined privacy broadly, observing that it will often be artificial to seek to distinguish between individuals' professional and private lives:

29. The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.

There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, 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. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.

To deny the protection of Article 8 on the ground that the measure complained of related only to professional activities - as the Government suggested should be done in the present case - could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them.

13. The Court went on to suggest that a search of any correspondence, whether professional or private, would necessarily engage Article 8. But the reasoning in subsequent cases has qualified this principle somewhat, giving more emphasis to the longstanding Article 8 concept of “reasonable expectation of privacy”.

14. *Halford v UK* (1997) 24 EHRR 523 concerned a senior police officer who had brought a sex discrimination claim. She claimed that the police had intercepted phone calls from her office for the purposes of gathering evidence to use against her in the proceedings, and that this violated Article 8. This was arguably a more difficult case because the telephone system in issue was the employer’s property, but on the particular facts the Court agreed that the calls were protected by Article 8. Its decision was based mainly on the absence of any warning that her calls might be intercepted:

There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex-discrimination case. (para 45)

Since there was at that time no provision in domestic law to regulate the interception of telephone calls made on internal communications systems operated by public authorities, the interference was not “in accordance with the law” as required by Article 8(2) and there was therefore a violation.

15. This decision has been interpreted as narrowing the protection of Article 8 in the employment context by enabling employers to defeat any reasonable expectation of privacy by giving a simple warning that calls might be intercepted. Applying the

decision in *Copland v UK* (2007) 45 EHRR 37, however, the Court held that telephone calls from business premises are “prima facie” covered by Article 8 and suggested that it will not be easy to rebut that presumption. *Copland* concerned an administrative employee of a state college, whose telephone, email and internet use were monitored by her employer. The government contended that the monitoring did not involve interception as in *Halford*, but merely recording the numbers called and the time and duration of calls, and equivalent information about emails and internet use. The information was stored but not used for any disciplinary or other purpose. Even on the basis of the government’s case the Court found that the recording of the information constituted an interference with Article 8. This was despite the fact that the college could have obtained much of the information legitimately through other means (such as telephone bills). There were some aspects of the facts that indicated a slightly more intrusive form of monitoring had taken place – such as contacting the recipients of calls or emails to discover their purpose – but this does not appear to have formed part of the Court’s (extremely brief) reasoning.

16. As in *Halford*, the interference was held to violate Article 8 because of the absence of any provision in domestic law regulating such monitoring.
17. The reach of Article 8 in the public sector workplace is therefore broad, especially as regards correspondence, but the test of “reasonable expectation of privacy” still gives scope to employers who give adequate warnings of monitoring to argue that Article 8 is not engaged at all. Such warnings, however, cannot be determinative since there must be some matters which are so inherently private (e.g. medical or legal correspondence) that a mere warning by an employer that they might interfere would not displace the expectation of privacy.
18. Article 8(1) also entails positive obligations on the state to protect against excessive privacy intrusion by private bodies⁷, but these are inevitably weaker than the negative obligation on public authorities not to interfere with privacy rights without justification and have not been held to extend to providing civil or criminal remedies for privacy intrusions in the private sector workplace.

⁷ See, e.g., *Von Hannover v Germany* (2006) 43 EHRR 7

PARTICULAR ISSUES ENGAGING PRIVACY RIGHTS AT WORK

Monitoring of correspondence

Regulation of Investigatory Powers Act

19. The decisions in *Halford* and *Copland* give rise to potential claims against public authority employers under Article 8. However the violation in both cases stemmed from the absence of any legal basis for the inferences in domestic law, a position which has now been corrected by the introduction of RIPA. Interferences made in accordance with the Act are likely to be justified under Article 8(2).
20. Until the introduction of the Interception of Communications Act 1985 there was no statutory regulation of the interception of communications (other than some specific offences regarding postal employees and interference with postal communications). The 1985 Act was introduced following the European Court's decision in *Malone v UK* (1991) 13 EHRR 448 which held that the absence of domestic law regulating police interception of telephone calls violated Article 8, but it did not cover interceptions on private telecommunication systems.
21. RIPA extended regulation to private systems and was intended to build human rights safeguards of necessity and proportionality into the authorisation of surveillance. However it granted extremely broad access to highly intrusive surveillance powers to a wide array of public authorities without any judicial oversight, and in the employment context it permitted interception of communications with very little restriction.
22. Lord Bingham has called RIPA "perplexing" and said that the House of Lords had difficulty construing it with confidence⁸. Undeterred, the following is a summary of the relevant provisions in the employment context.
23. Section 1(3) of RIPA creates civil liability for the interception of communications "without lawful authority" over a private telecommunications system (such as a

⁸ *AG's Reference (No. 5 of 2002)* [2004] UKHL 40 at para 9

company telephone and email system), whether internal or external calls/emails.⁹ Either the sender or the recipient of the communication can bring proceedings under this provision.

24. “Interception” is defined in section 2:

(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he—

- (a) so modifies or interferes with the system, or its operation,
- (b) so monitors transmissions made by means of the system, or
- (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

Because the act must occur “in the course of transmission” of the communication, it will only qualify as an interception if it involves opening a communication which has not yet been read. So accessing stored emails or text messages is not covered. Further, at least some of the *contents* as opposed to the mere fact of the communication must be disclosed. It is arguable that a subject header in an email would be sufficient to satisfy this requirement.

25. Under section 3, however, lawful authority for the interception will exist where the interceptor has reasonable grounds for believing that both the sender and the recipient consented to the interception. It is not clear how specific this consent must be. It might be possible, for example, for an employer to argue that a general term in a contract or collective agreement is sufficient to give reasonable grounds to believe the parties have consented.

26. More significantly, section 4(2) enables the Secretary of State to make regulations to authorise:

⁹ Note that section 1(1)-(2) also makes unauthorised interception a criminal offence

...any such conduct described in the regulations as appears to him to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record of—

- (a) communications by means of which transactions are entered into in the course of that business; or
- (b) other communications relating to that business or taking place in the course of its being carried on.

It is under this provision that the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (“the Lawful Business Practice Regulations”) were introduced.

27. Hazel Oliver’s 2002 article in the ILJ¹⁰ contains a fascinating examination of the political background to the Regulations, and in particular the extent to which the limits on email and telephone monitoring were watered down during the consultation process. In the event the Regulations provide very little restriction on employers.

28. Regulation 3(1) provides that interception for is authorised for the purposes of section 1 of RIPA if it is done for the purpose of:

- (a) monitoring or keeping a record of communications—
 - (i) in order to—
 - (aa) establish the existence of facts, or
 - (bb) ascertain compliance with regulatory or self-regulatory practices or procedures which are applicable to the system controller in the carrying on of his business or applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures, or
 - (cc) **ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties**, or
 - (ii) in the interests of national security, or
 - (iii) for the purpose of preventing or detecting crime, or
 - (iv) **for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system**, or
 - (v) where that is undertaken—
 - (aa) **in order to secure, or**
 - (bb) **as an inherent part of, the effective operation of the system** [...]; or
- (b) monitoring communications **for the purpose of determining whether they are communications relevant to the system controller’s business** [...]; or

¹⁰ “Email and internet monitoring in the workplace: information privacy and contracting-out” ILJ 2002, 31(4), 321-352

(c) monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

Employers are therefore able to monitor emails and telephone calls without consent for quality control purposes, or to check for unauthorised use of the system, or in order to protect the system against viruses, or simply in order to check whether the communication is a business communication. Pursuant to Regulation 2, “business” includes the activities of government departments and other public bodies.

29. Regulation 3(2) purports to provide some additional safeguards, but they are so widely drawn as to be of limited practical use:

Conduct is authorised by paragraph (1) of this regulation only if—

(a) the interception in question is effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller’s business;

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business;

(c) the system controller has made **all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted**; and

(d) in a case falling within—

(i) paragraph (1)(a)(ii) above [national security cases], the person by or on whose behalf the interception is effected is a person [authorised to apply for an interception warrant];

(ii) paragraph (1)(b) above, the communication is one which is intended to be received (whether or not it has been actually received) by a person using the telecommunication system in question.

30. The requirement to make all reasonable efforts to inform employees that their communications may be intercepted appears to mirror the “reasonable expectation of privacy” test in Article 8, but the difference in focus is significant. It is effectively a lower threshold, so it is conceivable there will be cases where on the facts an employee has a reasonable expectation of privacy notwithstanding the employer’s reasonable efforts to inform staff that their communications may be intercepted. The effect of the Regulations is to authorise interception in such cases without any requirement to satisfy the tests of necessity or proportionality.

31. In the case of public sector employers there remains some limited scope for claims under the HRA by employees whose correspondence is intercepted – either if the employer falls foul of the Regulations (because the interference would then not be “in accordance with the law”) or if it can be shown that the interference with Article 8 is not necessary or proportionate notwithstanding compliance with the Regulations. This avenue is only available, however, to those employed by “pure” public authorities. Hybrid bodies would not be subject to the HRA for these purposes because the monitoring of employees’ communications would not be considered a public function (see section 6(5) of the HRA). Hybrid and private sector employees will only have a remedy under section 1(3) of RIPA if an employer has failed to comply with the Regulations.

Data Protection Act

32. The monitoring of communications is very likely to constitute processing of employees’ personal data under the DPA, so the requirements of the Act must also be met.

33. Paragraph 6(1) of Schedule 2 of the DPA provides that processing will satisfy the First Data Protection Principle (processing must be fair and lawful) if it is “necessary for 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”.

34. Although this provision theoretically incorporates Article 8 ECHR, the remedies under the DPA are weak. A claim for compensation for unlawful processing can only be made if the data subject has suffered damage as a result (section 13). Mere distress cannot be compensated, unless the data subject has also suffered damage. The only other remedy is a complaint to the Information Commissioner, who has a discretion to issue an enforcement notice.

35. The Employment Practices Code issued by the Information Commissioner in June 2005¹¹ contains well-balanced guidance on the monitoring of employees' communications and advocates impact assessments to determine whether the likely benefits justify the any adverse impact. This goes some way beyond the requirements of the DPA, however, and is likely to be adhered to only by the most diligent of employers.

Directed covert surveillance

36. Many employers use the services of private agencies to investigate employees – usually those who have brought personal injury claims or who are on long term sick leave. This is likely to be highly intrusive, but there are very few legal safeguards against oppressive use of the practice.

Public authorities

37. Although this type of surveillance would appear to come squarely within the definition of directed surveillance under RIPA, the Investigatory Powers Tribunal (“IPT”) has held that covert surveillance of employees does not come within RIPA and therefore it does not have jurisdiction to consider such complaints.

38. Section 26(2) of RIPA provides:

Subject to subsection (6) [exemption for the enforcement of TV licensing], surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken—

- (a) for the purposes of a specific investigation or a specific operation;
- (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

39. The rest of Part II of RIPA provides for the authorisation of such surveillance by certain public bodies, including the police.

¹¹

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf

40. The applicant in *C v The Police and the Secretary of State for the Home Department* (2006) IPT/03/32/H [2006] Po. LR 151 was a police sergeant who had retired on medical grounds following an accident at work. His claim for damages had been settled for £100,000 and he was in receipt of additional pension benefits as a result of his injury. The police force for whom the applicant had worked instructed a firm of private enquiry agents to observe the applicant because they had suspicions about whether he was as disabled as he claimed. The firm took 9 minutes of video footage of the applicant mowing his front lawn in the presence of his wife and 9-year-old son, and filmed him in his car. No authorisation under Part II of RIPA was obtained.
41. The applicant brought proceedings in the IPT claiming that this was directed surveillance which was not authorised under RIPA and therefore violated his Article 8 rights.
42. The IPT held that the definition of “directed surveillance” was implicitly limited by the context of the legislation. RIPA created a regime of self-authorisation by public authorities for specified purposes which are related to their particular public functions. Not all public authorities are entitled to rely on all of the grounds available for authorising directed surveillance. For example, the police can rely on nearly all of the grounds (national security, preventing or detecting crime, in the interests of the economic well-being of the country), whereas local authorities are limited to surveillance for the purpose of preventing or detecting crime or of preventing disorder.
43. Since the employment of staff was common to all public authorities, the IPT considered it would be anomalous if some public authorities were covered by RIPA for surveillance for this purpose but others would not. On this basis they concluded that surveillance will only come within RIPA if it relates to the “core functions” of the public authority concerned, rather than to “ordinary functions” common to all public authorities.
44. The consequence of this is that covert surveillance of employees by public authorities for the purpose of investigating or defending claims of injury or ill-health is

likely to violate Article 8 because of the absence of legal safeguards (cf. *Halford* and *Copland*, above), unless (perhaps) express provision is made for it in the contract of employment.

45. It must follow that *McGowan v Scottish Water* EATS/0007/04 was wrongly decided by the EAT. The case concerned an employee of a water treatment plant who was subjected to covert surveillance to establish whether he was falsifying time sheets. He argued that his employer's actions violated Article 8 and that his dismissal on the basis of evidence obtained through the surveillance was therefore unfair. The EAT held by a majority that the interference with Article 8 was proportionate and therefore lawful, but it did not address the question of whether it had been done "in accordance with the law" under Article 8(2). Had it done, it would have been bound to conclude that there was no legal basis for the surveillance and it had therefore violated Article 8. Since the EAT implicitly considered that, had there been a violation of Article 8, the dismissal would have been unfair, that should surely have been the outcome on a proper analysis.

46. If public authority employers are to continue to conduct this kind of surveillance, further legislative regulation is therefore required, preferably as part of a broader overhaul of RIPA¹², in order to meet the UK's obligations under the Convention.

Private employers

47. Unless the surveillance amounts to harassment or some other tort, there is no cause of action against private employers who conduct directed surveillance of this kind. It ought to be possible, however, to rely on Article 8 in any resulting proceedings by virtue of the obligation on courts and tribunals to act compatibly with Convention rights.

48. First, any dismissal based on evidence obtained in breach of Article 8 should not be held to be "reasonable". This appears to have been the assumption of the EAT in

¹² See Liberty's response to the Home Office consultation on RIPA: <http://www.liberty-human-rights.org.uk/pdfs/policy-09/liberty-s-response-to-the-ripa-consultation.pdf>

McGowan, and in a slightly different context it was also accepted as the correct approach in *X v Y* [2003] UKEAT 0765_02_1106.

49. Secondly, the fact that evidence is obtained in breach of Article 8 may have procedural consequences. In *Khan v UK* (2001) 31 EHRR 1016 the European Court held that evidence obtained in breach of Article 8 may be admissible in criminal proceedings, and that this did not violate Article 6 (fair trial). The Court considered that the central question was whether the proceedings as a whole were fair, and that the court's discretion to exclude the contested evidence under section 78 of PACE was sufficient to protect against the risk of substantive unfairness.

50. This issue was examined in the context of civil proceedings in *Jones v University of Warwick* [2003] EWCA Civ 151. The claimant had brought proceedings against her employer, claiming damages for personal injury to her right hand. The defendant admitted liability but disputed that the claimant was still suffering from any disability. The defendant's insurers hired an inquiry agent, who obtained access to the claimant's home by posing as a market researcher, and filmed her using a hidden camera. The defendant claimed that the footage proved the claimant had entirely satisfactory function in her right hand. The claimant argued that by virtue of section 6 of the HRA the court was obliged to exclude the evidence because it had been obtained in a way that violated Article 8.

51. The Court of Appeal strongly disapproved of the insurer's conduct:

If the conduct of the insurers in this case goes uncensured there would be a significant risk that practices of this type would be encouraged. This would be highly undesirable, particular as there will be cases in which a claimant's privacy will be infringed and the evidence obtained will confirm that the claimant has not exaggerated the claim in any way. (per Lord Woolf CL at para 23)

52. The Court accepted that it was obliged to act compatibly with Article 8, but emphasised that the contravention in this case was that of the insurer's inquiry agent, not of the Court. It considered that any decision to admit evidence made pursuant to the CPR, if that entailed an interference with Article 8(1), would necessarily be justified under Article 8(2). On the issue of how to exercise its discretion, the Court held:

The court must try to give effect to what are here the two conflicting public interests. The weight to be attached to each will vary according to the circumstances. The significance of the evidence will differ as will the gravity of the breach of art 8, according to the facts of the particular case. The decision will depend on all the circumstances. (para 28)

53. In the event, however, there is little indication that the Court conducted a proper balancing exercise, saying that it could not “ignore the reality of the situation”. It concluded that this was not a case where the conduct was so outrageous that the defence would be struck out. Since the case therefore had to be tried, it was considered to be “artificial and undesirable” for the evidence not to be placed before the judge.
54. Instead the Court showed its disapproval by ordering the defendant to pay the costs of resolving the admissibility issue. This sanction is realistically unlikely to deter employers from adopting such evidence-gathering techniques. First, their primary concern will always be to succeed in defending the claim and they will know that any probative evidence is very likely to be admitted. It is difficult to see how a court could take a different view in any other case where relevant evidence was obtained. Secondly, although the costs in that case may have been substantial, because there were two appeals on the admissibility issue, in future cases courts will simply apply the Court of Appeal’s decision so either the point will not arise, or the costs of an application to exclude evidence will be minimal.
55. This does not go far enough to protect against what is arguably the most serious kind of privacy intrusion. If the Court of Appeal is right that the obligations under section 6 of the HRA cannot override the court’s discretion to deal with cases justly under the CPR then legislative intervention may be required. At the very least, it would seem reasonable to require employers to conduct some kind of necessity and proportionality assessment before undertaking covert surveillance of this kind. There is no reason why the sanction for non-compliance could not be the exclusion of evidence in a case as serious as *Jones*. Courts are often obliged to exclude relevant evidence where there are good public policy reasons for doing so (for example due to legal professional privilege, or public interest immunity). A penalty in costs is

simply too weak to deter employers who may be facing claims for damages substantially in excess of any adverse costs award.

Video surveillance on work premises

56. The use of CCTV cameras in the workplace is increasing as dramatically as in other spheres, and yet astonishingly there are still no statutory rules which apply specifically to the use of CCTV cameras – even those used by the police or other public bodies. The coalition government has promised to rectify this, but in the meantime the DPA and Article 8 are the only legal protections available, both of which have inevitable limitations for this purpose, particularly in the private employment sector.
57. CCTV used to monitor employees will be subject to the DPA. Fair and lawful processing requires giving employees adequate information about who will be processing the data, how it will be stored, and what its purposes are. The data must not be used for any purpose other than that specified by the employer, and it must not be processed in a manner incompatible with that purpose. So if an employer claims that CCTV is necessary to protect their property, it must not use it in a way which undermines that purpose, such as by not securing the data properly or allowing others access to it. The data captured must be relevant, not excessive to the purposes for which they are processed, and must not be kept for longer than is necessary. There must also be appropriate safeguards against unauthorised processing.
58. The requirement to avoid unwarranted violations of privacy in the First Data Protection Principle (see above) also means that the use of cameras in areas where there is a reasonable expectation of privacy would have to be justified on Article 8(2) grounds. CCTV in bathrooms, for example, is likely to breach the DPA (as well as giving rise to a potential Article 8 claim in the case of a public authority employer).
59. Although the Employment Practices Code again stresses the need for an impact assessment to determine whether the benefits of CCTV justify the adverse impact, the problems of enforcement identified above are equally applicable here.

Physical searches and testing

60. Although the Employment Practices Code deals with the handling of *information* obtained from drug and alcohol testing, there is no regulation of the conduct of tests themselves, or of physical searches of employees, e.g. to guard against theft of company property.

61. But since such testing or searches cannot be said to be an inevitable aspect of the employment relationship, they certainly require employees' consent otherwise the employer may be committing an assault. The more difficult question is whether an employer would be justified in taking disciplinary action against an employee who refuses to consent to a test or a search.

62. There have been no appellate cases on this point, but following *Gillan* in the European Court, even a superficial search of a person and their belongings could engage Article 8, and compulsory drug testing certainly does¹³. For the same reasons as set out above in relation to directed covert surveillance, a decision to dismiss for refusing to consent to a search which is not justified on Article 8(2) grounds ought to be held unfair.

Biometric security

63. Similar considerations should apply to fingerprinting or other forms of biometric tests used to identify employees. Public sector employees may have a freestanding claim under the HRA if such measures are not proportionate (cf. *S & Marper*), and private sector employees may be able to rely on Article 8 in the context of an unfair dismissal claim. This will obviously not assist employees who are required to consent to the measures as a condition of taking up an offer of employment, but it may provide some protection to long term employees who object to new measures being imposed upon the workforce.

¹³ See, e.g., *Peters v Netherlands*, decision of 6 April 1994

Activities outside work

64. Although the courts have acknowledged that disciplinary action on the basis of employees' activities in their private lives may engage Article 8, they have tended to accept that employers are entitled to take action, even where the connection to the employee's duties is remote¹⁴. These cases are worthy of reconsideration in the current climate, where Facebook and other internet-based socialising has created a huge reservoir of information that employers can access about their employees' private lives. The Law Society sensibly warned businesses last year that the information will not always be reliable, and that using such information could lead to discrimination claims.
65. There may well also be freedom of expression issues to consider: it is arguable that tribunals would have to construe any express or implied contractual term concerning public statements by employees compatibly with Article 10, so that a dismissal for posting a comment on Twitter or some other public forum would only be fair if it could be shown to be justified under Article 10(2).
66. Employees now have better remedies against third parties involved in vetting processes. A full examination of the law relating to criminal records checks and other vetting systems is outside the scope of this paper, but it is worth noting that privacy rights are now being afforded greater weight in this area.
67. In *R (Wright) v Secretary of State for Health* [2009] 1 AC 739 the House of Lords held that provisional listing on the Protection of Vulnerable Adults ("POVA") list may engage Article 8 because of the potentially serious consequences for care workers. Compliance with Article 8 therefore required that they be given an opportunity to make representations before provisional listing.
68. And in *R (L) v Metropolitan Police* [2010] 1 AC 410 the Supreme Court held that Chief Constables are required to give greater consideration to privacy rights when deciding whether to disclose non-conviction information as part of an Enhanced

¹⁴ See, e.g., *Saunders v Scottish National Camps Association Ltd* [1981] IRLR 277 and, more recently, *Pay v UK* (2009) 48 EHRR SE2

Criminal Record Check. Similarly, if there is any doubt as to the relevance or proportionality of a disclosure the applicant ought to be given an opportunity to make submissions.

69. It was hoped that the creation of the Independent Safeguarding Authority (“ISA”) would resolve both of these problems by creating a single independent system capable of adjudicating fairly without prejudicing employment prospects, but the Enhanced Criminal Record Check regime remains in place (and the guidance in *L* is often not followed), and the new Vetting and Barring Scheme (“VBS”) was due to run in parallel with it from November 2010. In June, however, the coalition government announced that the VBS has been put on hold pending a government review, due to concerns that the intended scheme was overly burdensome and unduly infringed on civil liberties.

CONCLUSION

70. Apart from being excessively complicated (and therefore largely inaccessible) the law regulating employers’ conduct in this area is inadequate to prevent or deter serious intrusions of workers’ privacy. There is no logical basis to distinguish between private and public sector workers for this purpose (as the IPT recognised in the *C* case), and therefore the availability of freestanding claims under Article 8 is arbitrary.
71. Although there are still few cases on point, the section 6 HRA duty on courts and tribunals should require them to incorporate Article 8 considerations into any assessment of the reasonableness of a dismissal. This indirect remedy, however, is not sufficient. Only workers who have the right to claim unfair dismissal are protected, and even they would have to resign and claim constructive dismissal in order to enforce their rights, a step that few employees are willing to take (hence, presumably, the lack of case-law on the issue).
72. What is required is a purpose-specific legislative scheme which provides for Article 8 protection for all workers, whether public or private sector. Now that the

issue of privacy is top of the political agenda (albeit in a different context) this may be the time to introduce such a regime.

CORINNA FERGUSON

LIBERTY

12 SEPTEMBER 2010