# I SPY…ISSUES RAISED BY THE SURVEILLANCE OF EMPLOYEES

**Julian Allsop, Guildhall Chambers**

## Introduction

1. There has always been a tension between the rights of an employee to privacy and the rights of an employer to gather information on the employee's performance and conduct.

2. Some methods of monitoring, such as time clocks, have been an accepted feature of the workplace since the latter half of the nineteenth century. However, other more modern forms of vetting, monitoring and surveillance are controversial and present challenges to the employer who would like to gather intelligence on its workforce, whilst not breaching the rights of its employee and the legal obligations that it is subject to.

3. Employees also gather information about their employers, particularly if they wish to set up in competition with their employer, or for the use in actual or contemplated legal proceedings. For instance, the reader is likely to be familiar with the scenario of the employee who secretly records a disciplinary meeting in order to protect and possibly enhance his position in relation to his employer. The questions that arise in each instance are how can this evidence be legitimately gathered, retained and deployed? Will the employee do more harm to his cause than good?

4. The line has to be drawn somewhere. This paper examines where it might lie during the currency of the employment relationship and during litigation.

**The Overarching Principles**

5. In any case involving surveillance in the employment context, it is necessary to consider the extent to which the following legislation is applicable:

   (a) The Data Protection Act 1998;

   (b) RIPA and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;

   (c) Article 8 ECHR as incorporated into English law by the Human Rights Act 1998.

**The Data Protection Act 1998**

6. The Data Protection Act 1998 ('DPA') applies to personal data, which can include that information processed in relation to disciplinary and grievance proceedings. In the case of ***Durant v Financial Services Authority*** [2004] IP & T 814[1], the concept of personal data under the DPA was held by the Court of Appeal to require it affect the individual's personal privacy whether in his personal or family life, business or professional capacity. The focus is on whether the information is biographical and whether it was information that had the data subject as its focus.

7. Whilst ***Durant v Financial Services Authority*** is regarded as the leading case on this issue, subsequent case law has suggested that it is not prescriptive of the only approach. In the case of ***Kelway v The Upper Tribunal*** [2013] EWHC 2575 Admin, the Court held that whilst ***Durant*** was starting point, in a more complex case it was one of a number of aspects to consider. Other relevant tests, which are suggestive of a broader approach included the definition of 'personal data' in the European Data Protection Directive, the WPO test[2] and the TGN test[3]. In the case of ***Edem v Information Commissioner and another*** [2014] EWCA Civ 92 it was held that a person's name (unless it was so common that it required a further work related identifier) was their personal data under the DPA.

8. With this concept in mind, we turn to the cardinal principles of the DPA regime (known as the Data Protection Principles) which are contained in Schedule 1, Part 1 of the DPA. There are eight Data Protection Principles.

9. The first, and probably the most important Data Protection Principle is that personal data shall be processed fairly and lawfully and , in particular, shall not be processed unless-

   (a) At least one of the conditions in Schedule 2 is met, and

   (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

10. Schedule 2 DPA contains the conditions relevant for the purposes of the First Data Protection Principle, namely the processing of any personal data. Schedule 3 sets out the conditions pertaining to the processing of sensitive personal data. 'Sensitive personal data' is defined by section 2 DPA 1998 and includes data consisting of information as to the racial or ethnic origin of the subject, his beliefs, health and criminal record.

11. Schedule 1 Part II DPA is the interpretation provision that supplements Part I. Paragraph 1 of Part II states that in determining for the purposes of the First Data Protection Principle whether personal data are processed fairly, regard is to be had to the method by which they

[1] Butterworths Intellectual Property and Technology Cases.
[2] This is a reference to Opinion WP136 dated 20th June 2007 of the EU Article 29 Working Party, which is the body that advises the European Commission on data protection.
[3] Technical Guidance Note on Determining Personal Data, dated 21st August 2007 issued by the ICO. It contains a checklist of eight matters which would assist with the determination of whether something is personal data or not.

are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

12. Paragraphs 2 to 4 of Schedule 1 Part II DPA requires, amongst other things, the employer data controller to make information readily available to its employees as to the identity of the data controller, the purpose or purposes for which the data are intended to be processed, and any further information which is necessary having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

13. Schedule 2 DPA sets out six conditions applicable to the processing of personal data. These include the consent of the employee (data subject) and five other circumstances, which are essentially where the processing of data is necessary for the compliance with a legal or other legitimate purpose.

14. The DPA extends to the retention of employment data and the monitoring of employees at work and is supplemented by Parts 2 and 3 of the Information Commissioner's Data Protection: Employment Practices Code (2011). This Code is not legally binding but may be referred to in any proceedings alleging a breach of the DPA.

15. Parts 2 and 3 of the Code should be carefully read by all employment practitioners. However, for the purposes of this paper, it should be noted that amongst the practice guidance in Part 2 includes provisions at paragraph 2.l3 that relate to the application of the DPA to discipline, grievance and dismissal proceedings. For instance, if there are unsubstantiated allegations, these should be removed unless there are exceptional reasons for retaining some record of them.

16. Part 3 of the Code is specific to monitoring at work. The core principles (paragraph 3.1) are:

    (a) It will usually be intrusive to monitor workers;
    (b) Worker have legitimate expectations that they can keep their personal lives private and that they are entitled to a degree of privacy at work;
    (c) Employers who wish to monitor their workers should be clear about their purpose and should be satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered;
    (d) Workers should be aware of the nature, extent and reasons for any monitoring unless (exceptionally), covert monitoring is justified; and
    (e) Workers' awareness will influence their expectations.

17. Impact assessments should be carried out before any monitoring activity is implemented to determine whether it is justified. An impact assessment involves:

    (a) Identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver;
    (b) Identifying any likely adverse impact of the monitoring arrangement;
    (c) Considering alternatives to monitoring or different ways in which it might be carried out;
    (d) Taking into account the obligations that arise from monitoring; and
    (e) Judging whether monitoring is justified.

18. Paragraph 3.2 of Part 3 of the Code sets out guidance in relation to the monitoring of telephone, fax, email, voicemail, internet access and other forms of electronic communication. The key points are that an organisation should decide whether to have an electronic communications monitoring policy, it should be reviewed to ensure that it is up to date with relevant data protection principles and up to date with practice in the workplace, and that the workforce is aware of them. Monitoring should not be conducted in such a way that would infringe the Regulation of Investigatory Powers Act 2000 (also known as RIPA).

19. Paragraph 3.3 of Part 3 of the Code sets out the guidance in relation to video and audio monitoring. The key points from this part of the Code are that any video or audio monitoring

should be targeted at areas of particular risk and confined to areas where expectations of privacy are low, and that continuous video or audio monitoring of particular individuals is only likely to be justified in rare circumstances. Workers and visitors should be given clear and adequate notifications that video or monitoring is being carried out.

20. Paragraph 3.4 of Part 3 of the Code sets out the guidance in relation to covert monitoring. In relation to this part of the Code, the guidance states that covert monitoring is an exceptional measure and that senior management should normally authorise any covert monitoring. This should be done where they are satisfied that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection. Covert monitoring should be strictly targeted at obtaining evidence within a set timeframe and should not continue after the investigation is complete. It should not be used in areas where workers would usually expect privacy. Information obtained by covert monitoring should only be used for the purpose for which it was collected. Any other information collected during the covert investigation should be disregarded and if feasible, deleted, unless it reveals information no employer could reasonably ignore.

21. If a private investigator is engaged to collect information on employees in a covert manner, it is necessary to make sure that a contract is in place that requires the private investigator to only collect information in a way that satisfied the employer's obligations under the DPA.

22. Supplementary Guidance to this Code has also been published and provides further assistance in relation to the statutory regime associated with the monitoring and interception of communications.

**Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

23. If an employer intends to monitor electronic communication such that it will involve the interception of communications in the course of their transmission, the Regulation of Investigatory Powers Act 2000 (also known as RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 are likely to apply.

24. RIPA prohibits the interception of a communication in the course of its transmission unless an employer has lawful authority to do so on the basis of a reasonable belief in the consent of the sender and recipient or there is a Court Order, or it is otherwise authorised by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. If RIPA is infringed, the offender may face criminal and civil penalties.

25. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide lawful authority for employers to access and monitor their own systems for standard business purposes such as maintenance of an IT system or to ascertain the extent of compliance with its IT policies and procedures. Whilst the employee's express consent is not required, it is a pre requisite to a lawful exercise of this right for users of the system to be notified.[4]

26. Further, before any steps are taken it may be necessary to consider whether the accessing of the employee's computer or data held on the computer is a breach of section 1 of the Computer Misuse Act 1990, which provides for a criminal penalty in the event of unauthorised access.

**Article 8 ECHR**

[4] 'Users of the system' in this context means employees of the organisation rather than third parties (e.g. those sending emails to the organisation), according to the Information Commissioner's guidance on the matter.

27. Article 8 of the European Convention on Human Rights was incorporated into UK Law by the Human Rights Act 1998. It ensures an individual's right to respect for his private and family life, his home and correspondence. It is a qualified right. Interference with this right is justified where it 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."*

28. It is applicable to public authorities, which includes the Courts and Tribunals who are tasked with determining issues that sometimes involve the balancing of competing rights, some of which are protected by the European Convention on Human Rights. It is also potentially applicable to a third tier of public authority, namely 'hybrid public authorities' which carries out partly public / partly private duties, in so far as it carries out functions of a public nature.

29. The Employment Tribunal is not competent to adjudicate upon any freestanding claim of a breach of Article 8, but as it is a public authority under s.6(3) of the Human Rights Act 1998, it is required to act in a way that is compatible with Convention Rights. As such it will be called upon to consider whether Article 8 has been engaged as part of the balancing exercise that it will have to carry out in determining the admissibility of evidence and the impact of any relevant breach of Article 8 on matters within its competence, such as the fairness of a dismissal, see further ***X v Y*** [2004] IRLR 625 at paragraph 53 *et seq*.

30. Whilst an employee may not have a claim under the Human Rights Act 1998 against a private sector employer, any claim that he brings is likely to be determined in accordance with all of the applicable legal principles, including if necessary, potentially applicable Human Rights. See ***X v Y*** at paragraphs 55 -58 and 63, also ***Turner v East Midlands Trains*** [2013] IRLR 107, in which the Court of Appeal indicated a higher standard of investigation (within the range of reasonable responses) would be placed on the employer in an unfair dismissal case where Article 8 interests were engaged.

31. Article 8 entered the UK workplace in the case of ***Halford v United Kingdom*** [1997] IRLR 471. In this case, Ms Halford's employer (a public authority, Merseyside Police) intercepted her telephone calls from her home and from her workplace. It was held by the European Court of Human Rights that the calls that were made to her from the workplace (in circumstances in which she had not been warned that her calls were being monitored and would therefore have a reasonable expectation of privacy) were capable of engaging the concepts of 'privacy' and 'correspondence'.

32. In the case of ***Copland v United Kingdom*** [2007] IP & T 600, the European Court of Human Rights held that Ms Copland, who had worked in a state run college, had her Article 8 rights infringed by her employer's collection and storage of personal information relating to her telephone, internet and email usage. As with Ms Halford's case, the fact that Ms Copland was not warned of the possibility of this monitoring by her employer led the Court to the view that she had a reasonable expectation of privacy, and it did not matter to the overall analysis of the case that her this personal data had not been otherwise disclosed or used against her in disciplinary proceedings.

33. In addition, it should be noted that depending upon the circumstances in which interception is taking place and the purposes for which it is being conducted it is possible that the employer's actions may constitute a breach of the relationship of trust and confidence. It is also conceivable that a disciplinary investigation predicated on a breach of these provisions, or in breach of the ECHR could be procedurally unfair.

**Considerations arising when there is surveillance by the employer**

34. There are myriad ways that an employer can monitor its employees. These include:

    (a) Physical Surveillance (inside and outside of the workplace);

    (b) Telephone monitoring, such as by recording telephone calls or reviewing telephone records;

    (c) Email and Instant Message Monitoring;

    (d) Internet log reviews, such as the review of browser data;

    (e) Social media surveillance;

    (f) Digital surveillance, for instance by the installation of software on an employee's workstation to ascertain precisely how and when the machine is being used.

**Physical Surveillance / Video Surveillance**

35. Video surveillance by the employer of the employee in the workplace, typically by the use of CCTV cameras, is *prima facie* lawful and does not engage Article 8, so long as it does not infringe a reasonable expectation of privacy.

36. There may nevertheless be a breach of the DPA in relation to the nature of the retention and processing of the data gathered. In order to avoid this outcome, as above, the collation and storage of the data gathered by CCTV monitoring must be in accordance with paragraph 3.3 of Part 3 of the Code. Before it is undertaken there should be an impact assessment within the meaning of the Code. The video monitoring should be targeted at areas of particular risk and confined to areas where expectations of privacy are low, and that continuous video or audio monitoring of particular individuals is only likely to be justified in rare circumstances

37. Covert video surveillance outside of the workplace presents some difficulty. Whilst the mere taking of a photograph (without any aggravating features) of another in a public place is unlikely to be actionable (see paragraph 36 of ***Wood v Commissioner of Police for the Metropolis*** [2009] EWCA Civ 414) as it would not usually attain 'a certain level of seriousness' to engage Article 8(1) in circumstances where there might be a 'reasonable expectation of privacy'[5], there nevertheless is the potential for interference with the employee's Article 8 ECHR rights when the employer that undertakes a campaign of covert surveillance is a public authority within the scope of the ECHR jurisprudence.

38. For instance, in the case of ***McGowan v Scottish Water*** [2005] IRLR 167, Mr McGowan was suspected of falsifying timesheets. His employer, Scottish Water, considered placing cameras in the workplace but decided that was impractical so decided instead to undertake covert surveillance of his home. Private Investigators were employed, who secreted themselves outside Mr McGowan's front door. They filmed his movements during the course of a week. Video footage was presented to his employers which confirmed their suspicions and Mr McGowan was dismissed.

39. He complained that his dismissal was unfair as his right to private and family life had been breached. The Employment Tribunal dismissed his claim on two bases, firstly that the covert surveillance had taken place from a public road and what was observed by the investigators could have been observed by any member of the public using the road. Secondly, that the employer's actions were justified under Article 8(2) in the light and nature of the offence that was being investigated.

[5] See also paragraphs 13-14 of ***City and County of Swansea v Gayle*** UKEAT/0501/12/RN.

40. By a majority, the Employment Appeal Tribunal dismissed Mr McGowan's appeal. It was concluded that covert surveillance of an employee's home raised at least a strong presumption that Article 8(1) was being infringed, but that in the circumstances of this case the measures that had been taken were proportionate and thus justified. The dismissal was fair.

41. A similar result was reached in the case of ***City and County of Swansea v Gayle*** [2013] IRLR 768. In this case, Mr Gayle was suspected by his employer of playing squash at a local sports centre whilst he was supposed to be at work. It conducted covert surveillance of him which confirmed their suspicion that he was claiming remuneration for working hours that he was not entitled to. He was summarily dismissed. The Employment Tribunal found that the covert surveillance was a breach of his Article 8 and the DPA Code. He was therefore unfairly dismissed but was awarded nil compensation.

42. The EAT disagreed with the Employment Tribunal's conclusion. Article 8(1) was not engaged. Not only could Mr Gayle not have a reasonable expectation of privacy at his local squash club, he certainly could not expect it when he was supposed to be working, and in the course of commissioning a criminal act, i.e. fraud.

43. Further, the finding that the covert surveillance was in breach of the DPA Code and thus unfair could not stand, as the Code was merely guidance as to what amounted to good DPA practice. It was not a substitute for consideration of the DPA itself, in relation to which no breach had been identified which would otherwise have made the dismissal unfair.

44. It was observed that there was no known authority where filming of an individual had been held to be a breach of Article 8 or the Human Rights Act where the filming had been conducted in a public place and there had been no alleged breach of RIPA.

45. Employers should be careful not to jump to conclusions about the surveillance evidence that they have gathered. In the well-publicised Employment Tribunal case of ***Pacey v Caterpillar Logistics Services (UK) Ltd*** ET 3501719/10, the Claimant who was off sick from work and was claiming sick pay had been observed by the employer's private investigator carrying a small shopping bag, walking the dog and clearing ice from his car. This led to his dismissal on the grounds of gross misconduct. The only medical opinion that was considered was a cherry picked report from the Claimant's General Practitioner, which was based on a narrative that had been provided to him of the video footage. The dismissal was held to be unfair.

46. The key point that this case highlights is that where video surveillance evidence is relied upon in disciplinary proceedings against an employee who is accused of malingering, it would be advisable for the actual surveillance footage to be analysed by an appropriately qualified medical professional before any conclusions are drawn about the employee's conduct.

47. Further to the preceding paragraph, the same point can also be made in relation to surveillance evidence obtained in the context of disability discrimination claims, particularly where disability is in issue.

48. Employment Tribunals are also called upon to determine the admissibility of evidence adduced in breach of the employee's Convention Rights per the Human Rights Act 1998, DPA and other relevant legislation such as RIPA.

49. In this respect, there is no real distinction between the principles applied in the Civil Courts and in the Employment Tribunal. In the case of ***Jones v University of Warwick*** [2003] 3 All ER 760, video evidence obtained by a private investigator who posed as a market researcher to gain access to Ms Jones' home was held to have been obtained contrary to Article 8. Even though the evidence had been obtained in clear breach of Article 8, the primary question before the Court in relation to the admissibility of this evidence was whether or not fairness and the interests of justice required its admission, and this was answered in the affirmative.

The Court's disapproval of the way in which the evidence had been obtained could be met by a suitable award of costs.

50. Sometimes, the balance between privacy and the interests of justice can be met by a suitable case management order, including pursuant to Rule 50 of the Employment Tribunal Rules 2013, which is stated in terms to be applicable in cases where it is necessary to protect the Convention Rights of any person. For example, in the case of ***XXX v YYY*** [2004] IRLR 137, in considering whether a covertly obtained video should be admitted as evidence, it was viewed by the Employment Tribunal in private, so as to protect the rights of a minor who was shown in the footage. (In the end, the evidence was not admitted as it was not relevant to the pleaded issues between the parties.)

**Telephone monitoring**

51. Monitoring telephone calls made by employees can potentially engage the DPA, RIPA and Article 8 ECHR.

52. The first matter to consider is whether the monitoring (and more pertinently, the personal data gathered thereby) is in line with the First Data Protection Principle in Schedule 1 DPA, which requires consideration of whether the criteria set out in Schedule 2 (for personal data) or Schedule 3 (for sensitive personal data) have been met. Usually, for Schedule 2 personal data, it will involve examination of the employment contract and other personnel documentation to determine whether consent has been given by the employees to the processing, or whether one of the other criteria, such the protection of the employer's legitimate interests, has been established. By this stage, an impact assessment should have been carried out.

53. Simultaneously, as telephone monitoring in the workplace is likely to involve the interception of communications that engages RIPA, it will be necessary to determine whether there is lawful authority to intercept the telephone communications. This will be established if the person intercepting has reasonable grounds for believing it has the consent of the sender and the intended recipient of the communication or the interception is authorised by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (i.e. if it is done for the purpose of accessing and monitoring their own systems for standard business purposes such as maintenance of an IT system or to ascertain the extent of compliance with its IT policies and procedures and the employee has been previously notified of this possibility).

54. As for Article 8, the effect of cases such as ***Halford v United Kingdom*** and ***Copland v United Kingdom*** is that where monitoring by public authorities has taken place without prior and sufficiently specific warning, that in such cases there would be a breach of Article 8. Private sector employers will have to consider this matter in the context of how an Employment Tribunal might approach the question of fairness under s.98(4) ERA 1996, if there is a dismissal.[6]

55. It should also be noted that in ***Copland v United Kingdom***, the European Court of Human Rights did not accept the argument that the analysis of telephone records did not engage Article 8, as the use of information relating to the date, length of conversation and numbers dialled were an important aspect of the telephone communication.

56. In determining admissibility, the same principles apply as are set out in the preceding section. In the case of ***Morison v Avocet Hardware plc*** [2003] All ER (D) 126 (Jul) the EAT held that the Employment Tribunal had erred in not admitting relevant evidence that was obtained in breach of RIPA, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, and that the interception of the telephone call amounted to a breach of Article 8 ECHR. It was pointed out that even if the evidence had been adduced in breach of a relevant statutory regime, there was normally a route to claim redress. This did

[6] See paragraphs 29-30 above.

not involve interfering with the interests of justice by the exclusion of otherwise relevant evidence.

**Email and Instant Message Monitoring**

57. The same issues as apply in relation to telephone monitoring also apply with the necessary modifications to Email and Instant Message monitoring. Further, ***Copland v United Kingdom*** also involved email and internet monitoring, with the same result that Article 8 was infringed by the employer's conduct. Similarly, the storage of this personal data also engaged Article 8(1).

58. Paragraphs 3.2.8 and 3.2.9 of the DPA Code should also be borne in mind, namely that the opening of emails should be kept to a minimum, particularly those that are marked private or personal and that monitoring should be kept to a minimum of address and heading unless it is necessary to open them to examine their content. Where practicable, ensure that those that send emails to the workers as well as the workers themselves are aware of the monitoring and the purpose behind it.

59. As for admissibility before the Employment Tribunal, even if an offending email has been obtained in breach of an Article 8 right this will not be determinative of the question. In the recent judgment of ***Atkinson v Community Gateway Association*** UKEAT/0457/12/BA, at paragraphs 67-69 the EAT affirmed the approach in ***Morison v Avocet Hardware plc***. Where there is an admissibility issue in these circumstances, it will be necessary for the Tribunal to carry out a balancing exercise which involves consideration of all relevant factors, including the probative value of the evidence in question and the nature and extent of the activity which has infringed the right of privacy.

**Internet Usage / Social Media / Digital Surveillance**

60. The same issues as apply in relation to telephone monitoring also apply with the necessary modifications to Internet usage, social media monitoring and digital surveillance. In relation to social media monitoring, there are likely to be issues arising under Article 8 ECHR and the DPA in relation to the tracking of an employee's digital footprint in cyberspace, and the storage of the information gathered as a consequence of that surveillance.

61. Digital surveillance (which can log key strokes, mouse clicks, clipboard activity, screen shots, search words inserted into browsers *et cetera*) are a relatively new technology that is developing at a fast pace. Given the intrusive nature of these technologies, employers would be well advised to strictly adhere to the standards set out in paragraphs 3.2 and 3.3 of the DPA Code.

**<u>Considerations arising when there is surveillance by the employee</u>**

**Secret Recordings**

62. The employer is also entitled to protection on public policy grounds where there is a reasonable expectation of privacy. For instance, in the case of ***Chairman and Governors of Amwell View School v Doghery*** [2007] IRLR 198, Mrs Doghery was subject to disciplinary proceedings that resulted in her dismissal for gross misconduct.

63. She secretly recorded the both the disciplinary proceedings at which she was present, and private deliberations of the Governing Body on the charges laid against her. She sought to adduce the transcript of these recordings in the Employment Tribunal. The Employment Tribunal determined that the evidence should be received. The Employment Appeal Tribunal partially allowed the employer's appeal. It determined that whilst the transcript of the

recording of the disciplinary hearing at which she was present should be admitted, the private deliberations should not be.

64. The Employment Appeal Tribunal based this judgment on the public policy grounds (paragraphs 72-73 of the Judgment), that parties before disciplinary and appeal proceedings should comply with the ground rules of such proceedings, and that a fundamental ground rule was that the deliberations of the panel should remain private, so as to encourage the full and frank exchange of views. This public policy consideration trumped the policy that a party to proceedings should be able to avail themselves of any relevant evidence.

65. However, the Employment Appeal Tribunal did not consider that the Governing Body's private deliberations engaged Article 8. As the panel members had put themselves forward into a public role by being Governors, there was no basis for considering that they nevertheless retained a right to personal privacy in the discharge of those public functions.

66. The *ratio* in ***Chairman and Governors of Amwell View School v Doghery*** was followed in the analogous case of ***Williamson v Chief Constable of the Greater Manchester Police and another*** UKEAT/0346/09/DM. The fact that this case involved a disability discrimination claim as opposed to an unfair dismissal claim did not make a difference to the application of the public policy considerations outlined in ***Chairman and Governors of Amwell View School v Doghery***. A similar view (i.e. that the fact that a recording is made covertly should not of itself result in its exclusion from evidence) was expressed in ***Vaughan v London Borough of Lewisham and others*** UKEAT/0534/12/SM.

67. ***Chairman and Governors of Amwell View School v Doghery*** **was distinguished in the recent** EAT judgment in ***Punjab National Bank (International) Ltd and others v Gosain*** . In this instance, the covert recordings of the 'private' elements of the interwoven disciplinary and grievance proceedings were held to be admissible as the nature of the comments fell well outside the area of legitimate consideration of the matters that fell to be considered by the grievance and disciplinary panels respectively. This included an instruction to dismiss the Claimant, and an admission that the grievance panel were deliberately skipping parts of the grievance. These matters therefore were not part of the deliberations in relation to the atters under consideration.

## Conclusion

### From the Employer's perspective

68. In general, an employer is entitled to carry out surveillance in the workplace, and in some instances outside of the workplace. However, surveillance in the workplace is fraught with difficulties. At all times, surveillance should be legitimate, proportionate and transparent.

69. Thus, if you are acting for an employer, at all times you should bear in mind your client's obligations under:

(a) The DPA, Schedule 1, in particular in relation to the specific situations contemplated by Part 3 of the DPA Code. As a matter of good practice:

(i) The starting point is the paperwork. Check that your client has the necessary policy framework to conduct the type of surveillance that it wants to do. Employment contracts and policies should be updated to ensure that the workforce is aware of the nature and extent of monitoring, and the legitimate interests that the employer is trying to protect.

(ii) It would prudent in all cases to carry out an impact assessment, and where covert monitoring is considered, have a clear audit trail to demonstrate that it was been the subject of conscientious decision at the level of higher management.

(iii) Monitoring (particularly covert monitoring) and the retention of data obtained thereby should be carried out to the minimum extent necessary to achieve the employer's aims.

(iv) If a third party investigator is to be used, ensure that the investigator is reputable and that there are adequate contractual safeguards in place so that there is compliance with the standards set out in Part 3 of the DPA Code.

(b) RIPA and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, and if there is the necessary element of consent and / or notification to avoid falling foul of these provisions.

(c) Article 8 ECHR. Even if your client is not a public authority within the scope of the Human Rights Act 1998, it would be prudent to act in a manner which is compatible with Article 8 ECHR, and thus not intrude where there would be a legitimate expectation of privacy. This will enhance your client's prospects of relying on surveillance evidence before the Employment Tribunal. Advise your client against undertaking an unnecessarily intrusive approach to investigation.

70. These standards and guidelines apply equally when investigating the activities of departed former workers who have moved on to a competitor or who have set up in competition with your client.

71. In most cases, the existence of covertly obtained evidence should be made known from an early stage in litigation so as to avoid any unnecessary delay and possible adverse cost consequences, should it be necessary to amend pleadings or adjourn hearings due to it coming to light at a late stage.

**From the Employee's perspective**

72. Whilst it might be frowned upon by the Employment Tribunal, it is permissible to secretly record disciplinary and grievance proceedings. However, it is likely that an Employment Tribunal will accede to an application to exclude evidence that has resulted from the covert recording of private deliberations, unless those discussions are not in substance deliberations of the underlying disciplinary or grievance proceedings.

    (By the same token, employers should ensure the propriety of the private deliberations to avoid any embarrassment caused by the admission of covert recordings).

73. Both sides might wish to avail themselves of a private hearing under Rule 50 of the 2013 Rules to determine the admissibility of controversially obtained evidence, or suggest hearing the evidence under Rule 50 as a gambit in order to tip the public policy / ECHR convention balance in its favour.

**Julian Allsop**
**Guildhall Chambers**
**September 2014**

The material contained in this article is provided for general information purposes only. It does not constitute legal or other professional advice. No responsibility is assumed by any member of chambers for its accuracy or currency, and reliance should not be placed upon it. Specific, personal legal advice should be obtained in relation to any case or matter. Any views expressed are those of the editor or named author.