

## Employee surveillance: what are the limits?

Employees face increasing amounts of surveillance by employers seeking to protect commercial interests or arm themselves with evidence in the event of litigation. Whatever stance one might take as to the rights and wrongs of such intrusive conduct, there is no denying that employee surveillance has the potential to produce hugely helpful evidence for use in litigation.

Akhlaq Choudhury reports

The benefits of surveillance to an employer are obvious: secret filming of an employee may establish that a disability does not have the adverse effect claimed and monitoring emails may confirm suspicions that an employee is acting in breach of confidence.

However, surveillance cannot be undertaken without regard to the limits imposed by various pieces of legislation, including the Data Protection Act 1998 (DPA), and rights conferred by article 8 of the European Convention on Human Rights (right to private and family life) and the Human Rights Act 1998.

Practitioners need to be aware, not only of these limits, but also of their own professional responsibilities when faced with a client eager to make use of surveillance to obtain evidence and the extent to which any evidence so obtained is likely to be admissible in court.

There is a vast range of activities that could be described as “employee surveillance”. Here, we focus on just two of the activities commonly faced by employment lawyers: covert video surveillance and monitoring email communication.

### Is covert video surveillance lawful?

Video surveillance at work – through the use of CCTV, for example – is permissible. However, data protection issues arise since the processing of data (including video recordings) of an employee by the employer must be lawful and fair.

The Information Commissioner’s Office has produced an extensive code on workplace monitoring that identifies good practice recommendations in relation to video (and audio) monitoring. The key points to note are:

- an employer should consider whether the benefits of monitoring justify the adverse impact on employees
- employees should be made aware of the extent and purpose of video monitoring
- where possible, such monitoring should be targeted at areas of particular risk
- monitoring should be confined to areas where expectations of privacy are low.

The code also deals with covert video monitoring where the employee is unaware that this is taking place. Covert

monitoring might be justified where there are grounds for suspecting that criminal activity or equivalent malpractice is taking place, and where the employer is satisfied that notifying employees about the monitoring would prejudice the prevention or detection of such activities.

The code expects that such covert monitoring will be rare and establishes a number of safeguards where an employer considers that it may be justified. Covert monitoring:

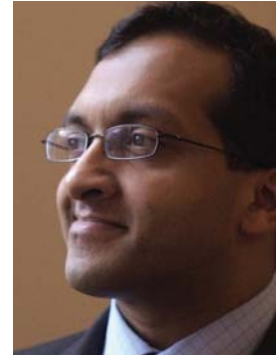
- should only be authorised by senior management
- should be strictly targeted for the purposes of a particular investigation
- should not take place in areas such as toilets that workers would genuinely and reasonably expect to be private.

The guidance above refers to workplace monitoring, but what about video surveillance outside work? Generally, this will involve the employer instructing an agency to obtain photographic or video evidence of an employee’s activities outside the workplace over a period of time.

Such surveillance is not contrary to common law per se and does not necessarily engage article 8 of the ECHR (see *C v Police and Secretary State for the Home Department* and *Wood v Commissioner of Police of the Metropolis*).

Data protection issues will also arise in relation to the processing of data obtained by such means. The code provides that if an agency is used in this way, the contract between the employer and the agency should ensure that the agency will only collect information in a manner that satisfies the employer’s obligations under the DPA. Indeed, it would be prudent to go further and ensure that any such contract provides that the agency will not engage in any unlawful means to carry out the surveillance.

Evidence obtained by means of deception or a trespass to gain access to an otherwise private environment will be unlawfully obtained and issues as to its admissibility may arise at a later stage (see below).



Akhlaq Choudhury:  
11KBW

**While the benefits of surveillance evidence may seem obvious or even overwhelming in a particular case, advisers need to ensure that clients understand that the means used to obtain and the use of such evidence must be lawful and fair**

The intrusive nature of covert filming means that article 8 may be engaged. Covert surveillance of a person’s home “raises at least a strong presumption that the right to respect for private life is being invaded and that article 8(1) is engaged” (*McGowan v Scottish Water*). The case added: “Whether a surveillance operation breaches the person’s right to have his private life respected is a question of proportionality”.

In *McGowan*, the surveillance was not considered to be disproportionate because the employee was suspected of falsifying time sheets and the employer needed to know whether those time sheets were being inaccurately recorded. By contrast, surveillance carried out on the “off-chance” of discovering misconduct is less likely to be considered proportionate.

**Is email monitoring lawful?**

Monitoring of emails is to be distinguished from the interception of live email traffic. The latter is regulated by the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and can only be undertaken in limited circumstances.

Monitoring of work-related emails that have already been sent or received and which are stored on the employer’s systems is permissible. However, as with video monitoring there are data protection implications. The code recommends that there should be an email policy in place that notifies employees that their communications may be monitored and sets out what types of communication would be unacceptable, for example, pornographic or discriminatory material.

Employees are entitled to have a reasonable expectation of privacy in relation to emails clearly marked “private and confidential” and there should not be routine monitoring of such emails. However, where there is suspicion of specific unlawful or criminal activity, it may be reasonable to monitor even private emails for a limited period. The code’s recommendations in respect of covert video monitoring also apply to the covert monitoring of private emails.

**Professional obligations**

The clearest obligation is that a barrister or solicitor must never advise that evidence be obtained illegally. Moreover, if the evidence has already been obtained illegally, no advice can be given that the evidence be updated or clarified in any way if to do so would involve a further illegal act. If evidence has already been illegally obtained, the client must be advised of his disclosure obligations.

Legal professional privilege does not attach to material obtained by means of a criminal or fraudulent enterprise: see *Dubai Aluminium co Ltd v Alawi* and *Hughes v Carratu International plc*. All such material obtained, its source and letters of instruction will have to be disclosed to the other side (see the Bar Council guidance, “Illegally Obtained Evidence in Civil and Family Proceedings”).

**Admissibility of surveillance evidence**

The fact that evidence has been obtained in contravention of the law will not in itself render such evidence inadmissible in court. In fact, the courts have taken a fairly robust approach to the use of evidence in such circumstances, tending to decide in favour of admitting evidence that is clearly relevant but expressing its disapproval of the means used to obtain it through the use of adverse costs orders: see *Jones v Warwick University*. The court would be more likely to exclude improperly obtained evidence where it is of marginal benefit to the case or where there was a very grave and unjustified infringement of article 8 rights.

As well as the costs risk, employers seeking to rely upon improperly obtained evidence face a further risk when seeking a remedy, such as an injunction, in that it could be said that the application is not being made with “clean hands”.

**Conclusion**

It will be apparent that this is an area where advisers need to tread with care. While the benefits of surveillance evidence may seem obvious or even overwhelming in a particular case, advisers need to ensure that clients understand that the means used to obtain and the use of such evidence must be lawful and fair. Where evidence has already been improperly obtained, there can be no guarantee that such evidence will be admitted by the court, and advisers need to take careful account of their professional obligations in advising or continuing to advise the client.

**Akhlaq Choudhury, 11KBW**

**Cases referred to:**

- C v Police and Secretary State for the Home Department* IPT/03/32/H
- Wood v Commissioner of Police of the Metropolis* [2008] EWHC 1105
- McGowan v Scottish Water* [2005] IRLR 167
- Dubai Aluminium co Ltd v Alawi* [1999] 1 WLR 1964
- Hughes v Carratu International plc* [2006] EWHC 1791 (QB)
- Jones v Warwick University* [2003] 1 WLR 954