

# Spy tactics

*Employers face a number of legal challenges if they use radio-frequency identification to monitor employees' movements, Susanne Foster warns*



*Susanne Foster is an associate at CM Murray LLP*

'Use of RFID technology is becoming so frequent that in May 2009 the European Commission provided guidance on designing and operating RFID applications in a "lawful, ethical and socially and politically acceptable way" that respects the right to privacy and ensures the protection of personal data.'

**R**adio-frequency identification (RFID) has the potential to revolutionise a business. It can increase efficiency and assist with managing logistics. However, concern has been expressed about the unscrupulous use of the technology to track employee activity and to accumulate and store a substantial amount of personal information.

There has also been alarm about the possible implantation of RFID tags under human skin. For example, the Health and Safety Executive's 'Scenarios Project' imagines a future where, by 2014, gangmasters are injecting workers with inventory tags to track their movements<sup>1</sup>. Although this may seem like an Orwellian fantasy, it is actually a reality (albeit not yet in the context of the workplace): one nightclub in Barcelona invites its members to have RFID chips implanted as a convenient way to gain VIP admission and pay for drinks<sup>2</sup>.

## The technology

RFID is a form of tracking technology that uses microchips not much bigger than a grain of rice. The microchips use electromagnetic energy to communicate wireless information as the chip passes a scanner. Although RFID chips are normally only read from a few feet or a matter of inches away, like a barcode, reports indicate that some tags can be read from a much further distance – from hundreds of metres<sup>3</sup> or even by satellites<sup>4</sup>.

Use of RFID technology is becoming so frequent that in May 2009 the European Commission provided guidance on designing and operating RFID applications in a 'lawful, ethical and socially and politically acceptable

way' that respects the right to privacy and ensures the protection of personal data<sup>5</sup> (see box on p19). However, despite the increasingly pervasive nature of devices equipped with RFID it is easy to forget the extent to which we are individually monitored.

At the moment, RFID technology is primarily used in supply-chain management, tracking vehicles between depots and pallets of goods from warehouses to stores. However, it has a multitude of uses. For example, Delta Airlines tags customer luggage, helping to reduce the number of lost bags and making it easier to route bags if customers change their flight plans<sup>6</sup>. ExxonMobil uses RFID technology for its 'SpeedPass', which instantly collects payment at petrol stations from a tag on a driver's keychain. RFID is also deployed in the Oyster cards used by the London transport system, in workplace security passes, payment cards for work canteens and passports.

The first commercial human-implantable RFID microchip was Verichip, marketed by Positive ID, after receiving approval by the US Department of Health and Human Services in 2004. About twice the length of a grain of rice, the chip is typically implanted above the triceps area of a person's right arm. The insertion procedure is performed under local anaesthetic in a doctor's office. According to Positive ID, the microchip does not offer tracking services as it does not have built-in Global Positioning System (GPS) support or long-range wireless communications.

Less physically invasive but no less controversial is the use of RFID chips in staff uniforms. In Sydney, Australia,

the Star City casino placed RFID tags in 80,000 employee uniforms to keep track of the uniforms. In Japan, employers use the technology to monitor how much each worker contributes to production<sup>7</sup>. Retailers such as Marks & Spencer and Tesco have in the past been accused of ‘dehumanising their workforce’ after research from the GMB union claimed that the use of electronic tagging of staff was on the rise<sup>8</sup>.

RFID technology is rapidly and continually advancing. The former Labour government had proposed using the technology in its controversial ID card scheme, and China is rolling out over one billion ID cards containing RFID chips.

**Security concerns**

‘Secure’ technology rarely stays as secure as the manufacturers claim. The RFID security in passports and ID cards has already been cracked, allowing hackers to extract information, including names, dates of birth and the passport-holder’s biometric information. The Oyster card security has also been defeated. All of this can be done from a distance, without even touching the passport or card. This has serious privacy and data protection implications (discussed further below).

**Health and safety**

Concern has also been expressed about the health and safety risks associated with RFID technology. The GMB has claimed that the technology is a source of exposure to electromagnetic radiation and that extensive use of hand-held scanners could also increase musculo-skeletal disorders. The only consistent messages from the scientific community are that research on possible health effects is inconclusive and that as long as transmitters (such as mobile phones and RFID technology) are below the limits set for static electromagnetic fields, the risk is low enough to be acceptable.

Nevertheless, until the medical position is clarified, employers have a statutory duty, imposed by the Health and Safety at Work etc Act 1974, to look after employees’ health and safety. In addition, under the Management of Health and Safety at Work Regulations 1999, the employer must:

... make a suitable and sufficient assessment of the risks to the health

and safety of his employees while they are at work.

**Negligence claims for psychological damage**

Employers will also need to consider the psychological consequences of tagging their staff and of staff regarding this as covert monitoring.

*Employees may feel less valued and even dehumanised if their every move is tracked. Arguably, if an employer does not trust them to do their job without being electronically monitored, this could breach the implied duty of mutual trust and confidence.*

In addition to the above statutory duties, employers have a common-law duty to take reasonable care of employees’ health and safety, including avoiding psychiatric injury caused by stress at work. To establish an employer’s liability, the harm to the employee must be reasonably foreseeable and the employer must have failed to take steps to prevent such harm.

An employer is entitled to assume that an employee can withstand normal job pressures unless it knows that an individual is particularly vulnerable. However, a case can be made that tagging staff is outside the boundaries of normal job pressure. If an employer fails to take steps to avoid psychological injury from the outset, it

may well face costly negligence claims for stress-related disorders.

Arguably, reasonable steps for an employer to take could include regular health checks or one-to-one meetings with employees. In this case, the additional management time involved in ensuring that an employer does not breach its duty

of care might outweigh the advantages of tagging that employee in the first place.

Any employer considering the use of RFID to monitor their workforce must thoroughly assess the possible health and safety risks in advance, as well as weigh up the commercial costs and benefits. The assessment should include both physical risks and the risk of employees developing stress-related illnesses as a result of their movement being constantly monitored.

**Other possible claims**

Employees may feel less valued and even dehumanised if their every move is tracked. Arguably, if an employer does not trust them to do their job without being electronically monitored,

**European Commission recommendation**

In May last year, the European Commission published *Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*. This recommends that member states ensure that RFID operators develop and publish a concise, accurate and easy-to-understand information policy for each RFID application. It also suggests the minimum level of detail which should be included in such a policy.

The recommendation also establishes that member states should require industry to develop a framework for privacy and data protection impact assessments, and sets out how the Data Protection Directive and EU Charter of Fundamental Rights should be applied to RFID chips.

Although Commission recommendations are not legally binding, the Commission does expect member states to take action on both new and existing RFID systems. The Commission is due to report on how the recommendation has been implemented in two to three years’ time. If necessary, it could then change its recommendation, propose further measures or replace the recommendation with hard legislation if its objectives are not being met.

this could breach the implied duty of mutual trust and confidence.

This duty implies a term into every contract of employment that neither the employer nor the employee will conduct themselves in a manner calculated or likely to destroy or seriously damage the relationship of confidence and trust between them, without reasonable and proper

data. Part 1.1(1) DPA 1998 defines personal data as:

... data which relate to a living individual who can be identified:

- (a) from those data, or
- (b) from those data and other information which is in the

- obtained only for specified and lawful purposes and not processed in any manner incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which it is processed; and
- subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

*If an employer required an employee to wear an RFID chip to locate them, and information about their comings and goings was stored on the tag and linked to a database containing personal data which identified that individual, DPA 1998 would apply.*

cause. It seems self-evident that tagging employees to check on their performance and/or conduct shows distrust and is not acting towards them in good faith.

Employers who breach the duty of mutual trust and confidence could face employee resignations and claims for constructive unfair dismissal (from employees with the requisite length of service). More worryingly, in terms of financial and reputational damage, if an employer tags specific categories of employees or uses tagging in certain departments or sectors in which one ethnic minority or sex predominates, this could expose it to costly claims of discrimination.

**Data protection**

The use of RFID tagging is likely to trigger the application of the Data Protection Act (DPA) 1998, which regulates the processing of personal

possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Therefore, if an employer required an employee to wear an RFID chip to locate them, and information about their comings and goings was stored on the tag and linked to a database containing personal data which identified that individual, DPA 1998 would apply. This would mean that any processing of personal data would need to be in accordance with the eight principles set out in schedule 1 to DPA 1998. These state, for example, that personal data shall be:

- processed fairly and lawfully;

The rather dated technical guidance from the Information Commissioner's Office (ICO) on RFID (published in 2006) does not address its use in the workplace in detail<sup>7</sup>. However, it refers the reader to the Information Commissioner's Employment Practices Code (the Code) for more detailed guidance on monitoring at work.

The Code itself, which was issued under s51 DPA 1998, deals with the impact of data protection laws on employment relationships and sets out recommendations on how to meet DPA 1998's legal requirements.

The Code has four parts, and Part 3 looks at data protection and the monitoring of employees at work. To ensure compliance with DPA 1998, the ICO recommends that employers carry out an impact assessment to decide whether monitoring is a proportionate response to the problem they seek to address and, if so, how to carry it out. An impact assessment in the RFID scenario would involve:

- identifying clearly the purpose or purposes behind RFID monitoring and the likely benefits;

**THE COMMERCIAL LITIGATION JOURNAL**

The bi-monthly journal designed to meet the needs of commercial litigators

For a FREE sample copy: call us on 020 7396 9313 or visit [www.legalease.co.uk](http://www.legalease.co.uk)



- identifying any likely adverse impact;
- considering alternatives to RFID monitoring or different ways to carry it out;
- taking into account the obligations that arise from monitoring; and
- judging whether the RFID monitoring is justified.

Any data obtained through RFID would need to be processed lawfully and fairly, and only used for specific, explicit and legitimate purposes. Employers would also need to have proper data protection and employee-monitoring policies in place, with effective audit processes and regular reviews to ensure that such systems were actually effective.

#### Human Rights Act 1998

Another piece of legislation emanating from Europe that may assist in preventing future abuse of RFID is Article 8 of the Human Rights Act (HRA) 1998. This provides that:

Everyone has the right to respect for his private and family life, his home and his correspondence.

Although not directly about RFID technology, the Scottish Employment Appeal Tribunal (EAT) case of *McGowan v Scottish Water* [2004] illustrates how Article 8 may provide a basis for challenging employer surveillance. In this case, the employer became suspicious that timesheets were being falsified and

did not represent what was actually happening. After considering various options, the employer decided to carry out covert surveillance on the employee. Precisely how this was done is not clear, although it seems that private investigators hid opposite the employee's front door and filmed him coming and going.

In determining that Article 8 was not violated, the Scottish EAT concluded that although the covert surveillance affected the employee's private and family life, in this case it was

*Although employers may be able to defend using surveillance to deal with a criminal threat, such as theft or fraud, they may find it harder to justify using it to deal with a more general perceived threat.*

proportionate because it was aimed at investigating specific, potentially criminal misconduct. However, although employers may be able to defend using surveillance to deal with a criminal threat, such as theft or fraud, they may find it harder to justify using it to deal with a more general perceived threat.

Although the UK courts are required as far as possible to interpret all legislation, whenever enacted, in a way that is compatible with the European Convention on Human Rights, the provisions of HRA 1998 only give rise to direct claims against public authorities. Therefore, the protection available to the majority of employees in private employment will be limited, as they will not have a standalone claim.

*McGowan v Scottish Water*  
[2004] UKEAT 0007/04/2309

#### The future

RFID undoubtedly offers a potentially powerful tool to improve employer operations. Employee monitoring is nothing new, but the rapid evolution of this technology poses difficult questions, as the law does not seem to have kept pace. Unless or until the law is changed to provide employees with specific protection on RFID

monitoring, employers need to be aware of employees' piecemeal employment rights, not least the right to privacy and protection under DPA 1998. Further, employers should think carefully about why they want to use RFID and how they will use the data gathered without provoking employee fears of unnecessary monitoring.

It is perhaps a useful exercise for legal advisers and the legislature to think about how RFID is likely to develop further in the workplace and what safeguards are necessary. In five or ten years, could it be common for employers to tag all of their staff invasively and monitor their every move? If so, it will be interesting to see in which legal arena the first cases emerge – will they be human rights, unfair dismissal, data protection or psychological damage claims?

On the other hand, as a nation we have generally shown a relaxed (or even naive) attitude to the invasive technology which constantly monitors our daily lives. A report from the House of Lords estimated that four million cameras are in use in Britain and confirmed that most experts agree that the UK leads the world in its use of CCTV<sup>9</sup>. It remains to be seen whether employees adopt an equally laissez-faire attitude to RFID, or whether implanting microchips in humans will be a step too far. ■

#### Reference point

1. [www.hse.gov.uk/horizons/scenarios/toughfull.pdf](http://www.hse.gov.uk/horizons/scenarios/toughfull.pdf)
2. [news.bbc.co.uk/1/hi/technology/3697940.stm](http://news.bbc.co.uk/1/hi/technology/3697940.stm)
3. [www.rfidjournal.com/faq/28/139](http://www.rfidjournal.com/faq/28/139)
4. The RFID chips that transmit information via satellite are not of the same nature or size as normal RFID tags. The US Department of Defence is using this technology to track supplies around the world.
5. [ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf)
6. Institute of Internal Auditors: [www.theiia.org/download.cfm?file=97597](http://www.theiia.org/download.cfm?file=97597)
7. [www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/radio\\_frequency\\_identification\\_tech\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_identification_tech_guidance.pdf)
8. [www.personneltoday.com/articles/2005/06/07/30224/gmb-claims-electronic-tagging-dehumanises-workforce.html](http://www.personneltoday.com/articles/2005/06/07/30224/gmb-claims-electronic-tagging-dehumanises-workforce.html)
9. [www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1805.htm#a22](http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1805.htm#a22)