Is Big Brother watching you? — CCTV surveillance at work

Davinia Brennan, Associate in the Litigation and Dispute Resolution department at A&L Goodbody, examines some of the issues which employers should consider before installing a CCTV system, in order to ensure compliance with the DPAs

CCTV surveillance is becoming increasingly prevalent in every aspect of our lives. Recognisable images of people captured by CCTV cameras constitute 'personal data' as defined in the Data Protection Acts 1988 and 2003 ('the DPAs'). Accordingly, all use of CCTV by employers must be undertaken in compliance with the DPAs.

Recent headlines such as 'Dunnes Stores employee sacked from her job after she was caught on camera eating €10 worth of chicken goujons' (*Irish Independent*, 26th February 2014) highlights the widespread use of CCTV for security purposes and for monitoring employees' performance, and raises questions as to whether such use is lawful.

This article examines some of the issues which employers should consider before installing CCTV systems, in order to remain compliant with the DPAs.

Obligations of employers

Transparency and proportionality are the key considerations to be taken into account by an employer before they install a CCTV system.

1. Transparency

The use of CCTV must be 'transparent'. Section 2(1)(a) and section 2D of the DPAs require personal data to be obtained and processed fairly, and for certain information to be supplied to an individual before their data are collected and processed. In order to comply with these provisions, an employer should notify employees and any clients or customers whose image will be captured on camera, of the use of CCTV cameras and the purpose for which they are used. Surveillance should only be carried out to give effect to the stated purpose and any ancillary use will most likely be unlawful.

The Data Protection Commissioner ('DPC') has published Guidance on CCTV ('the Guidance' — copy available at www.pdp.ie/docs/10037).

The Guidance suggests that the notification requirement can be achieved by placing easily-read and well-lit signs in prominent positions at all entrances. Where the usual purpose (i.e. security) for the CCTV is obvious, all that may need to be placed on the sign is that CCTV is in operation, as well as contact details (such as a phone number) for persons wishing to discuss the processing. This contact may be the security company operating the CCTV cameras, or the employer.

2. Proportionality

Section 2(1)(c)(iii) of the DPAs requires personal data to be adequate, relevant and not excessive for the purpose for which they are collected. This requires an employer to show that the installation of the CCTV is justified. The Guidance suggests that, whilst use of CCTV for security purposes is likely to meet the proportionality test, using CCTV to constantly monitor employees is highly intrusive, and would need to be justified by reference to special circumstances.

The location of cameras is also significant. The use of CCTV in places where employees would expect privacy, such as in bathrooms would be difficult to justify.

Using CCTV to monitor employees: The extent to which any monitoring of employees is lawful will depend on striking a fair balance between an employee's right to privacy and an employer's legitimate business interests. Employers should have a clear written policy on the monitoring and surveillance of employees. If employers intend to use CCTV for monitoring staff performance or conduct, then employees should be informed before their data are recorded for this purpose.

Employees also have a right to privacy under the European Convention on Human Rights and under the Irish Constitution. Whilst the latter does not expressly provide for a right to privacy, the courts recognise that the personal rights in the Constitution

(Continued on page 4)

(Continued from page 3)

imply the right to privacy. However, the right to privacy is not absolute, and may be limited or restricted in certain circumstances, such as for the legitimate interests of the employer.

The Annual Reports of the DPC contain Case Studies which provide an insight into some of complaints made to his office, and formal decisions made by him.

Case study 9/2011 demonstrates the unlawful use of CCTV to remotely monitor an employee's performance.

The employee complained to the DPC that he had received two written warnings from his employer, a Leisure Club, as a result of the use of CCTV, which had been installed without prior staff notification. The Club claimed that CCTV had been installed with the priority purpose being security, but due to complaints received from customers that the office was not open or was unattended, a secondary purpose of the CCTV was to monitor staff performance. It indicated that the cameras were overt, and that the staff were aware of the reasons behind the system.

The DPC made a formal decision that the Club had breached section 2(1)(c)(ii) of the DPAs by further processing CCTV footage, which was obtained for security purposes, in a manner incompatible with that purpose. The DPC stated that he would 'only expect CCTV footage to be reviewed to examine the actions of individual staff members in exceptional circumstances of a serious nature, where the employer could legitimately invoke the provisions of section 2A(1)(d) of the DPAs, (the processing is 'necessary for the purposes of the legitimate interests pursued by the data controller, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject').'

Top ten tips for operating CCTV systems in compliance with the DPAs

When using CCTV, in order to ensure compliance with the DPAs, employers should ensure that such systems:

- are transparent
- are fair, necessary and proportionate in respect of the concerns it tries to allay, and not excessive to the intended purpose
- strike a fair balance between an employee's right to privacy and an employer's legitimate business interests
- are carried out in the least intrusive manner possible

They should also ensure that:

- notice of the operation of CCTV and its purpose (s) is prominently displayed on the premises
- a clear written policy is in place for any CCTV surveillance of employees, which sets out the extent of surveillance and the purpose(s) for which it will be used, including its possible use in any disciplinary proceedings
- CCTV data are not kept for longer than necessary for the purpose(s) for which they were obtained
- CCTV data are protected against unauthorised access, disclosure or alteration
- any person whose image is recorded is given a copy of the information recorded upon request
- covert surveillance is only undertaken in limited circumstances, such as to prevent or detect crime, with the actual or intended involvement of An Garda Síochána

Covert Surveillance

Covert surveillance should only be undertaken in exceptional circumstances.

The use of covert CCTV, without an employee's knowledge, is generally unlawful.

The Guidance states that: 'covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to provide this evidence to An Garda Síochána.'

Case study 6/2007 illustrates the unlawful use of covert CCTV footage to terminate an employee.

The employer, a hotel, had installed covert CCTV cameras to investigate a complaint concerning cash handling at the hotel bar. The employee was not the subject of the investigation. No criminal prosecutions took place following the hotel's investigation, nor was the employee interviewed by An Garda Siochana. The DPC found that the hotel had unfairly obtained the employee's personal data through its use of covert surveillance. In addition, the hotel had breached the DPAs by further processing the employee's

personal data in a manner incompatible with the original purpose.

Using CCTV footage before the EAT

CCTV footage is used as evidence in cases before all levels of our court system, particularly before the Employment Appeals Tribunal ('EAT'). However, CCTV footage which has been obtained in breach of the DPAs cannot be lawfully used against an employee for internal disciplinary or EAT proceedings.

This is demonstrated by case study 10/2008, in which the DPC found that an employer could not rely on covert CCTV footage obtained in breach of the DPAs to pursue potential irregularities in attendance of two employees.

Nonetheless, unlawfully obtained CCTV footage is often relied upon by employers before the EAT in disciplinary matters. For example, covert footage was part of the evidence shown to the EAT in the case of *Kearney v Gresham Hotel Group Limited* UD891/2006. The reason that such footage is admissible before the EAT is due to the fact that, as a statutory body, it was established to deal with, and adjudicate on, employment disputes, and does not have any jurisdiction to consider data protection issues.

Other cases before the EAT, such as *Martin McGarrigle v Donegal Sports and Golf Centre Ltd* UD680/2002 and *McCollum v Dunnes Stores* (Oakville) Ltd UD424/2002 indicate that the question of admissibility of CCTV evidence depends on whether the claimant has been afforded the opportunity to view the CCTV footage and rebut any allegations against him/her.

However, employers should be aware that, in relying upon CCTV footage obtained in contravention of the DPAs for disciplinary purposes, they are at risk of being prosecuted by the DPC, and could be liable to a fine of up to €3,000 on summary conviction, or up to €100,000 on conviction on indictment.

Employee's right of access to CCTV footage

An employee whose image has been recorded has a right of access to a copy of the CCTV footage pursuant to section 4 of the DPAs unless a relevant exemption applies. In practical terms, a person should provide such information as the date, time and location of the recording to the data controller. If the image is of such poor quality so as not to clearly identify the employee, that image may not be considered to be personal data.

The recent case of *Dublin Bus v The Data Protection Commissioner* [2012] IEHC 339 shows that the courts will enforce a data subject's right of access to CCTV footage of him/her, even where legal proceedings are in existence between the data subject and the data controller. The High Court upheld an enforcement notice issued by the DPC obliging Dublin Bus to deliver a copy of CCTV footage to a data subject. The CCTV footage in question concerned an incident involving the data subject allegedly sustaining personal injury on one of its buses.

Obligations of security companies

A security company which operates a CCTV system on behalf of an organisation is a 'data processor' under the DPAs. Pursuant to section 2(2) and 2C of the DPAs, the security company and the organisation must enter into a legally binding agreement, providing that the security company will only act upon the instructions of the organisation and will implement all the necessary technical and organisational safeguards against accidental and unlawful forms of processing.

An organisation should further carry out due diligence to ensure the security company is complying with these obligations.

Retention of CCTV footage

Section 2(1)(c)(iv) of the DPAs requires that data must not to be kept for longer than is necessary for the purpose for which they were obtained. Therefore a data controller should be able to justify any retention period for CCTV footage. The DPC's Guidance indicates that it would be difficult to justify retention of CCTV footage concerning security for longer than one month, except where the images identify an issue such as a break-in or theft, and are retained for the purposes of an investigation of that issue. The footage should be stored in a secure environment, ideally with access restricted to authorised personnel, and an access log kept.

A summary of the ten top tips for how to remain compliant with data protection law whilst operating a CCTV system is available in the grey box on page 4.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com