Data protection and employment — Part 2

Striking the right balance between the privacy rights of workers and the legitimate interests of employers can be challenging. In this article, Oisin Tobin and Phillip Nolan, from Mason Hayes & Curran, explain how employers can overcome the particular challenges relevant to staff monitoring

Employers have a legitimate interest in preventing staff misconduct. Consequently, they generally wish to monitor the workplace activities of their employees.

However, employees do not lose their right to personal privacy when they walk through the office door. In *Copland v United Kingdom* (a 2007 case), the European Court of Human Rights found that an employee's right to respect for his or her private life and correspondence could be violated by an employer's monitoring of telephone calls, email correspondence and internet use.

This article considers how employers can deal with the specific challenges of CCTV, email/ internet monitoring and the use of private detectives.

Transparency

It is vital that any monitoring in the workplace is fair and transparent. In *Copland,* the European Court of Human Rights laid particular significance on the fact that the employee had been given no warning that her communications and internet usage were being monitored. It was this lack of transparency and knowledge that constituted an interference with her right to privacy.

This requirement for transparency is reflected in Section 2 of the Data Protection Acts 1988 and 2003 ('the DPAs'), which require among other things that personal data are obtained fairly for specified, explicit and legitimate purposes. The requirement is further underlined by Section 2D of the DPAs, which requires that a data subject is informed of the purposes of the processing and receives any other information necessary to make the processing substantively fair.

The *Copland* case and the statutory provisions above drive home the same basic point: employers must inform employees about any monitoring. Such notification should generally be provided via clear policies. Such policies should be written in plain English and should be provided to all new recruits, ideally with a copy of their contract of employment. Potential employees should be given an opportunity to review such policies, along with their proposed contract, prior to signing. Taking these steps will assist an employer in showing that the employee understood how their workplace activities could be monitored.

Basis for monitoring

It is not enough for employers to simply inform employees of the existence of workplace monitoring; employers must also be able to show that such monitoring can be justified under the DPAs.

Employers may, in the first instance, be tempted to assert that employees have consented to monitoring, either explicitly via signed policies, or implicitly by choosing to work with the knowledge that monitoring is taking place.

While consent usually provides a justification for processing under Section 2A of the DPAs, it is problematic in an employment context. The Article 29 Working Party, in both Opinion 8/2001 on the processing of personal data in an employment context and Opinion 15/2011 on consent, cast a serious doubt over the validity of consent in an employment context, noting:

An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid.

Employers may be tempted to solely rely on their contract with the employee, which may envisage monitoring, to justify workplace surveillance. However, relying on the 'necessary for the performance of a contract' justification for processing may be risky. It particular, it opens up the possibility of dispute as to whether or not a specific form of processing is actually 'necessary' under a given contract. In addition, it does not afford the flexible freedom of action that can be obtained by simply implementing proportionate monitoring in reliance

(Continued on page 4)

(Continued from page 3)

upon the legitimate interest ground for processing.

Therefore, in the absence of valid consent, an employer will likely need rely on its 'legitimate interests' to justify monitoring, which is a ground in Section 2A(1)(d) of the DPAs. However, Section 2A(1)(d) will not justify processing which is 'unwarranted in any particular case, by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject'. Consequently, any monitoring under Section 2A(1)(d) will need to balanced and measured.

Employers should:

- obtain formal written consent for any monitoring; but also
- ensure that any such processing is appropriate and sufficiently limited in scope so that it can be justified, in the absence of consent, by the legitimate interests of the employer.

Email and internet monitoring

Employers are entitled, in compliance with the DPAs, to monitor their employees' workplace email and internet use. However, to ensure that such monitoring is legal, it must be transparent and capable of being justified in light of the legitimate interests of the employer. This is the case, firstly, because it is too risky to solely rely on consent. Secondly, the DPC, in his guidance note on staff monitoring, specifically notes that the "main guiding principle is that you do not lose your privacy and data protection rights just because you are an employee. Any limitation of the employee's right to privacy should be proportionate to the likely damage to the employer's legitimate interests.

"These requirements can be met by drawing up a clear and fair 'acceptable use policy', governing the employees' use of electronic resources. This policy should be drawn to employees' attention during induction and, ideally, should also be reiterated whenever employees are accessing electronic resources."

These requirements can be met by drawing up a clear and fair 'acceptable use policy', governing the employees' use of electronic resources. This policy should be drawn to employees' attention during their induction and, ideally, should also be reiterated (ideally through a notification when the employee logs in) whenever employees are accessing electronic resources.

It is important to stress that an acceptable usage policy imposes limitations on the employer as well as the employee. Such a policy should explain how the employer can monitor the employee's online behaviour as well as setting out the permissible ways in which an employee can use resources. An employer cannot generally engage in additional monitoring over and above what is set out in the acceptable use policy. Such additional monitoring would lack transparency and could amount to the unfair processing of personal data.

The complete content of an acceptable usage policy requires a consideration of matters falling beyond the scope of data protection law. From a privacy standpoint, it is vital that such a policy expressly sets out the extent to which employee communications are monitored. Such policies should also set out any limits on the manner in which employees can use work facilities. For example, it should set out whether or not employees are entitled to use email for personal reasons, or whether non-work related web browsing is permitted.

CCTV

Closed Circuit Television, despite its ubiquity, poses particular data protection challenges. The Data Protection Commissioner ('DPC'), in his Guidance Note on CCTV, notes that employers should, prior to installing any CCTV cameras, consider the purpose of such surveillance.

As a general rule, the use of cameras for security reasons is acceptable. However, the DPC is of the view that the use of cameras for staff monitoring "is highly invasive and will need to be justified by reference to special circumstances". The use of such cameras as in strong rooms, or over cash machines, may be permissible. However, the use of cameras to calculate the length of staff coffee breaks is likely to cause problems.

The transparency principle in the DPAs requires that the purpose of CCTV surveillance is disclosed to employees. In particular, if cameras are being used for staff monitoring, this fact must be drawn to the employees' attention. Similarly, hidden cameras should generally not be used unless they are necessary to actively investigate potential criminal wrongdoing.

Employers should also bear in mind that, as CCTV images can constitute personal data, it may be necessary for such footage to be handed over in response to a subject access request. The use of CCTV footage for disciplinary purposes can be a fraught topic. Misuse of such images can potentially derail disciplinary proceedings. In Case Study 10 of the Guidance Note on CCTV, an employer used CCTV to monitor its employees' workplace attendance, and sought to use such evidence to justify disciplinary proceedings. The employees were never informed that the cameras would be used for staff monitoring. The DPC intervened and the employer had to drop the disciplinary proceedings.

A similar, but more serious, example occurred in Case Study 6 of 2007. As part of an internal investigation, a well-known Dublin hotel used concealed

cameras to monitor cash handling at its bar. The footage obtained from the cameras was then used to terminate a supervisor's employment. The supervisor was not the original subject of the investigation and no subsequent criminal investigation followed. The DPC took the view that use of the footage against an individual who had not been the original subject of the investigation, and the failure to be transparent with staff about the monitoring, amounted to a breach of the DPAs. The hotel was forced to agree a settlement with its ex-employee.

It is vital that an employer intending to use CCTV footage for staff monitoring informs its staff of this intention. While such an announcement may give rise to a complaint, particularly by workers' representatives, concealing the intention is self-defeating. If an employer is not upfront, not only may it encounter grave difficulties in using any CCTV footage in disciplinary proceedings, but also it may, by engaging in unfair processing, find itself to be in breach of the DPAs.

Private investigators

Surreptitious surveillance of staff by private investigators is a particularly high risk area. The Commissioner recently brought successful prosecutions against a number of insurance companies who used such investigators to obtain non-public social welfare information. The comparative rareness of data protection prosecutions in Ireland highlights the robust approach that the DPC is likely to take to the improper use of PIs.

In Case Study 14 of 2009 in the Guidance Note on CCTV use, an employer hired a private investigator to track one of its employees. The employee was a sales representative, and the employer wanted to ensure that the employee was properly discharging his duties. The investigator filmed the movements of the employee and his children for approximately one week. The employer was of the view that such monitoring was justified in the circumstances of the case.

However, the DPC took the view that the processing was not justified as the employer had failed to take any steps to highlight its concerns to the employee prior to hiring the investigator and recording his movements. The DPC further noted that "[c]overt surveillance of individuals is very difficult to reconcile with the Data Protection Acts." The DPC continued that such surveillance is unlikely to be legal, but as a minimum, there must be strong and evidence based justification for such surveillance in the first instance.

Employers must therefore exercise extreme care prior to the use of any private investigators.

Conclusion

Monitoring employees in a manner that is compliant with the DPAs is a comparatively straightforward process. The principles of proportionality and transparency are crucial. Employers should be fully transparent about the manner in which they monitor their employees' workplace activities. In addition, they should ensure that any monitoring is, in all respects, balanced and reasonable.

If employers follow these two basic rules, they stand a good chance of navigating through the thicket of challenges posed by workplace surveillance.

Philip Nolan and
Oisin Tobin
Mason Hayes & Curran
pnolan@mhc.ie
otobin@mhc.ie