Monitoring Employee Communications: Data Protection and Privacy Issues

By

Anthony Sakrouge, Kate Minett, Daniel Preiskel and Jose Saras

Reprinted from **Computer and Telecommunications Law Review**
Issue 8, 2011

Sweet & Maxwell
100 Avenue Road
Swiss Cottage
London
NW3 3PF
(Law Publishers)

SWEET & MAXWELL

Monitoring Employee Communications: Data Protection and Privacy Issues

Anthony Sakrouge
Partner, Russell-Cooke LLP, London

Kate Minett
Solicitor, Russell-Cooke LLP, London

Daniel Preiskel
Senior Partner, Preiskel & Co LLP, US

Jose Saras
Senior Associate, Preiskel & Co LLP, US

Data protection; Electronic communications; Employee monitoring; Interception of communications; Privacy; Proportionality; Right to respect for private and family life

Communications technology continues to develop rapidly and employee activities in the virtual electronic world of the internet and email can have very real consequences for employers. These range from embarrassment and reputational damage to practical problems, such as exposure to computer viruses, breach of confidentiality and potential legal liabilities for everything from discrimination to defamation. In light of this, it is understandable that so many employers want to take active steps to monitor their employees' electronic communications and internet activity. However, like any form of workplace monitoring, this necessarily raises issues of privacy: to what extent can employees expect their workplace communications to be treated as private and to what extent can an employee's work life be separated from his or her personal life?

Types of monitoring

Depending on the reason for the monitoring, employers might wish to monitor or intercept email content, email traffic, internet use and telephone use. This could include looking at the number, destination, source and content of emails, websites visited and destination, duration and content of phone calls.

Types of monitoring can also include one off spot checks, which look at communications across an organisation but which do not refer to individual usage, spot checks on individual employees and more continuous monitoring of organisational or individual usage, either on a targeted or random basis.

Expectations of privacy and data protection

One of the key questions that employers should examine when considering monitoring is the extent to which an employee has a reasonable expectation that any communications are private. What it will be reasonable for the employee to expect will depend both on the factual context (for example, the nature of the employer's business, the employee's role within that business and the nature and content of the communication) and the information given by the employer regarding the level of privacy that employees can expect for their workplace communications (for example, in an IT policy or staff handbook).

The idea of reasonable and informed expectation is central to the Data Protection Act 1998 ("DPA"). The DPA refers to "personal data" and "sensitive personal data". "Personal data" is data from which a living individual can be identified, either on the basis of the data alone or in combination with other information in the possession or likely to come into the possession of the person or organisation holding the data. "Sensitive personal data" is data which relates to specific aspects of an individual's life, including his or her racial or ethnic origin, religious beliefs or mental and physical health. Any "processing" of personal or sensitive personal data will fall within the scope of the DPA: for the purposes of the DPA, processing covers practically anything that an organisation would wish to do with data including organising, consulting, retrieving or destroying that data.

The monitoring of employee communications will necessarily involve the processing of personal, and sometimes sensitive, employee data. The first of the eight data protection principles set out in the DPA requires that data be processed "fairly and lawfully". In addition, the second data protection principle states that data should only be obtained for a specified and lawful purpose and shall not be processed in a manner incompatible with that stated purpose. In practical terms this requires employers to properly inform employees of any monitoring they plan to carry out.

Interception of communications

In the event that an employer is monitoring or intends to monitor the electronic communications of his employees, such employer would need to be aware of the requirements under the Regulation of Investigatory Powers Act 2000 ("RIPA 2000"), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[1] and the Computer Misuse Act 1990 ("CMA").

[1] Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699).

RIPA 2000 concerns the regulation of investigatory powers, such as interception, acquisition and disclosure of data or surveillance on private and public communications systems. According to RIPA 2000, an interception of a communication "in the course of its transmission" (query whether RIPA applies after the transmission ends) would be lawful if (i) a warrant is issued by the Secretary of State or a senior official; (ii) either the recipient and the sender consented to the interception or the interceptor has reasonable grounds for believing that the sender and the recipient had consented to the interception or (iii) the interception is requested for providing communication services. Employers should be aware that unlawful interception could lead to imprisonment, a fine, or both.

Furthermore, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, aims to strike a balance between the needs of the businesses and the rights of the employees. Therefore, such regulation includes several exceptions to the non-interception principles which would apply where consent is absent. Hence, by way of example, the interception of communications in a business environment would be allowed (i) "in order to establish the existence of facts"; (ii) to ensure compliance with standards and regulations by employees; (iii) for a system's security; (iv) for training, and (v) to prevent and detect crime. Such exceptions are construed narrowly, as they are mostly limited to business related communications and the controller has to make every reasonable effort to apprise the person who is using the system of the chance of interception.

Finally, employers should also be aware of the prohibitions under the CMA, as interception might amount to unauthorised access covered by the CMA. In fact, it seems that under the CMA an offence could be committed not only in the event of unauthorised access to computer material, but also when hacking into mobile phones or accessing their voicemails (a mobile handset could qualify as a computer as well as the servers in which voice messages are stored) and obtaining the tools necessary to perpetrate such offences. The penalties set out under CMA could be imprisonment, a fine, or both. Employees could also be entitled to civil remedies for breach of confidence and breach of data protection rules.

Clear policies consistently applied

Therefore, putting in place and implementing a clear IT policy regarding email, internet and telephone usage is essential for an employer to comply with the first two data protection principles that data be processed "fairly" and for a "specified purpose". The Employment Practices Code ("EPC") and accompanying Supplementary Guidance ("SG") issued by the Information Commissioner's Office (ICO) gives additional guidance on compliance with data protection legislation in the workplace. It states that any "rules and standards must be known and understood by workers"—IT policies should give clear and detailed information as to what the employer views as acceptable and unacceptable. In some cases employers may choose to ban any personal use by employees of work communication systems and internet access. Where some personal use is permitted, an employer should take care to set out what it considers to be acceptable in terms of material, level of usage and times of day when usage takes place. In an unreported case in the Aberdeen Employment Tribunal[2] two sisters were found to have been unfairly dismissed for excessive internet use on the basis that, in dismissing them, their employer had relied on a policy that was not sufficiently clear as to the level of internet use that was considered acceptable. Not only should such policies be clear, they must also be applied consistently. In *Robinson v Network IT Recruitment Ltd*[3] an employee was found to have been unfairly dismissed (even if a 15 per cent deduction in compensation was made for contributory fault) for sending an offensive joke by email where the circulation of such material was commonplace and where disciplinary action was not usually taken by the employer.

In addition, either in the policy or a separate document, the employer should set out its policy in relation to monitoring, including the:

> "circumstances in which monitoring may take place, the nature of the monitoring, how the information obtained through monitoring will be used, and the safeguards that are in place for the workers who are subject to monitoring."(SG 3.1.3)

Workers should:

> "be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained, how it will be used and who, if anyone, it will be disclosed to."(SG 3.1.4)

Consent

The first data protection principle requires that, in addition to being processed "fairly and lawfully", data can only be processed if one of a list of additional conditions is met. One of the conditions that organisations most commonly rely upon is that the individual concerned has consented to his/her data being processed.[4] However, there are potential difficulties for an employer who tries to rely on employee consent to the monitoring of his/her electronic communications. What constitutes valid consent is not defined in the DPA. Council Directive 95/46,[5] from which the DPA is derived, states that consent must be "freely given" and "unambiguous". Whether

[2] *Grant v Mitie Property Services UK Ltd* 2009.
[3] *Robinson v Network IT Recruitment Ltd* (2901763/04).
[4] DPA 1998 s.1, Sch.2.
[5] Directive 95/46 of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

consent can ever by "freely given" by an employee who wants to keep their job is questionable. In any case, it will not be possible for an employer to obtain prior consent to monitoring from third parties outside the organisation who email employees and whose data will also be captured by any communications monitoring that takes place. However, employers should endeavour to provide to third parties information regarding any monitoring that is taking place and how and why such monitoring is being carried out. This is usually done through recorded telephone messages and email footers. However, employers should note that this type of notification will not be enough to satisfy the "consent" condition in the DPA.

Impact assessment

Although it will not always be possible for an employer to rely on consent to show that it has complied with its data protection obligations when carrying out employee monitoring, it may be able to rely on the alternative condition that the processing is being carried out pursuant to the "legitimate interests" of the organisation or another party to whom the data will be disclosed.[6] Indeed, the EPC states that "employers who can justify monitoring on the basis of an impact assessment will not generally need the consent of individual workers." An "impact assessment" is a formal or informal process by which the employer examines the extent to which any adverse effects of monitoring on individuals is justified by any benefits to the employer or others. The ICO states that an impact assessment involves:

- "identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver
- identifying any likely adverse impact of the monitoring arrangement
- considering alternatives to monitoring or different ways in which it might be carried out
- taking into account the obligations that arise from monitoring
- judging whether the monitoring is justified." (EPC)

Where it considers monitoring to be essential, an employer should always consider ways in which the invasiveness of this monitoring can be minimised. This could include measures such as limiting the use of monitoring to use only in cases where allegations or complaints have been made, carrying out monitoring on a departmental rather than individual basis, automating monitoring so that personal information is not viewed by other workers who might know the individual in question, monitoring email headings or traffic rather than email content and using spot checks in place of continuous monitoring. Employers should also remember that they are obliged by the seventh data protection principle to ensure that any information gathered through monitoring is processed and stored securely. Employers who wish to send employee data for processing overseas should also be aware that the eighth data protection principle prohibits transfer of data to countries outside of the European Economic Area unless an "adequate" level of data protection can be guaranteed.

The "legitimate interests" condition which the impact assessment reflects is not available as a justification for the processing of sensitive personal data. However, sensitive personal data can be processed where this is necessary to comply with employment law.[7] As such, an employer might be able to show that monitoring an employee's emails was in compliance with the DPA where it was necessary to properly investigate an accusation of harassment or discrimination which would be in contravention of a worker's employment rights because there was no alternative method by which it could access this information.

Proportionality and human rights

The idea of proportionality and balancing the interests of different parties is central to the data protection impact assessment. It also underpins the Human Rights Act 1998 ("HRA") which incorporates much of the European Convention on Human Rights (ECHR) into UK law. Article 8(1) of the ECHR states that "everyone has a right to respect for his private and family life, his home and his correspondence". In *Halford v United Kingdom*[8] the ECrtHR stated that it was:

> "clear from case law that telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence within the meaning of Article 8 s.1'."

The ECrtHR confirmed that this also applied to emails sent from work and the monitoring of internet usage in *Copland v United Kingdom*.[9] Therefore, employers should not consider that employee communications in the workplace are necessarily public by virtue of their context and should assume that, regardless of information given to employees and policies in place, employees retain some entitlement to privacy in the workplace.

However, art.8 is not absolute and art.8(2) allows for derogation from the right to privacy where this is necessary in the:

[6] DPA 1998 s.6(1), Sch.2.
[7] DPA 1998 s.2(1), Sch.3.
[8] *Halford v United Kingdom* [1997] I.R.L.R. 471.
[9] *Copland v United Kingdom* (2007) 25 B.H.R.C. 216.

> "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 freedom of others."

In an employment context, the monitoring of employee communications will often be justifiable to protect the rights of other workers, or in some cases, the interests of the employer itself. The ECrtHR confirmed in *Pay v United Kingdom*[10] that in some circumstances, the protection of an employer's reputation will be justification for the infringement of the art.8 right. However, as with the ICO's emphasis on the need for employers to carry out an impact assessment before implementing any form of communications monitoring, proportionality is key. Any infringement of a worker's art.8 right to privacy will only be justifiable where that infringement is necessary for a legitimate aim which is significant enough to justify limiting the individual's rights and even then only if the individual's right is limited only to the extent absolutely necessary to achieve the aim. In practical terms this requires employers to ensure that any monitoring that they implement is essential to achieve a particular, justifiable outcome and that this outcome cannot be achieved through any less invasive means.

Employment relationship

An employer considering the monitoring of employee communications must give proper consideration to the external framework of legislation discussed above but must also bear in mind that employee monitoring can also raise issues that go to the contractual heart of the employment relationship. An employee who has not been properly informed that monitoring is taking place, or who feels that such monitoring is an unjustified invasion of their privacy may try to argue that the term of mutual trust and confidence which is implied into all employment contracts has been breached, and that he or she has been constructively dismissed as a result.

[10] *Pay v United Kingdom* [2009] I.R.L.R. 139.