

# E-MAIL MONITORING- I

## EAVESDROPPING AT WORK — IS IT LEGAL?

Mark Crichard

Recent events, relating to the circulation of a particularly personal E-mail, highlight once again the inherent risks associated with E-mail communications. Whilst the content of the E-mail concerned may not have been directly harmful to the relevant employers of the sender or the intended recipient, the situation also emphasises the delicate balance employers have to strike between accepting the reality that employees will often use work telephones, E-mail and Internet access for personal purposes and the need to protect their business interests. In this article we try to explain what businesses can and cannot do in terms of monitoring their staff — to reduce these risks — and summarize several of the relevant pieces of UK legislation which have an impact on such activities.

There are several pieces of legislation which affect this area, most notably the Data Protection Act 1998 (the DPA), the Human Rights Act 2000 (the HRA), the Regulation of Investigatory Powers Act 2000 (the RIP Act) and the recent Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the Regulations). Unfortunately, they are not always consistent with each other, as I shall explain below.

### THE RIP ACT

Until recently there has been very little guidance on when businesses could tap telephones or intercept or record E-mails. The interception of communications transmitted over public telecommunications network has for many years been regulated (and largely prohibited) by acts such as the Interception of Communications Act 1985 (the IOC Act). However, until now no specific rules applied to interceptions on private networks, which is where most businesses will monitor this sort of traffic.

The RIP Act, which came into force on 2nd October 2000, replaces the IOC Act and is wider in scope, extending the regime governing interception to both public and private telecommunications networks. As such it is an attempt to bring together all the relevant legislation on interception into one statute and to adapt those measures to reflect current communication methods, such as E-mail. The RIP Act also deals with many other related issues (such as access to encrypted messages and surveillance activities) which are not being addressed in this article.

In its first section the RIP Act makes it an offence (punishable by a fine and/or imprisonment) to intentionally and without lawful authority intercept communications without either the express or implied consent of both the sender and the recipient.<sup>1</sup> This offence applies equally to interceptions taking place over public and private networks, except in the case of interceptions on a private network by or with the consent of the network controller — in which case such an interception would amount only to a tort. The RIP Act does however provide a 'defence', in that an interception is treated as authorized (and

thus lawfully intercepted) if the interceptor has the consent of or reasonably believes that both parties (i.e. the sender and recipient) gave consent to such interception.<sup>2</sup>

These provisions have been amended by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the Regulations), which came into force on 24 October last year. The Regulations have been created pursuant to the power given to the Secretary of State under Sections 4(2) and 78(5) of the RIP Act. Specifically the Regulations seek to allow the interception of certain types of business communications on private networks, which would otherwise be prohibited under the RIP Act.

To rely on this, there are a number of criteria that have to be satisfied and the interception can only be made for one or more of the specified purposes. To begin with the interception must take place on a telecommunication system provided for "use wholly or partly in connection" with the business concerned; the interception must be solely for the purpose of monitoring or recording messages that are relevant to the business; and all reasonable efforts must be made to inform all actual and potential users of the relevant telecommunications system that messages may be intercepted. Obviously this latter requirement does not require the need to obtain specific consent from the relevant senders/recipients for particular interceptions or recordings, as consensual interception is not itself prohibited under the RIP Act. However, it is up to individual businesses to determine what may or may not amount to reasonable efforts to alert.

In addition, interceptions will only be authorized under the Regulations if they are for one or more of the following purposes:

- (a) monitoring or keeping a record of communications in order to (amongst other things):
  - establish facts
  - ensure compliance with applicable regulatory or self regulatory practices
  - demonstrate the standards that should be achieved relating to, for example, quality control and training
  - prevent crime

- investigate unauthorized use of telecommunication systems
  - secure an effective system operation
- (b) monitoring communications in order to determine whether they are business or personal communications.

It therefore seems that it is legitimate under the Regulations to monitor E-mails, for example, to protect a network from viruses or to ensure employees do not breach company rules or policies. Likewise, in relevant cases businesses may intercept calls or E-mails for the purposes of quality control or staff training. However, until the Regulations are tested out in the real world there are some obvious areas of possible confusion or uncertainty.

The most glaring issue is the extent to which the Regulations allow monitoring and presumably reading of (or listening in to) E-mails or other communications marked as 'private' or which are clearly personal for the purposes of ascertaining whether they are in fact business related. Where an employee has a concern over the activities of a particular individual this may be exactly what needs to be done to identify a misdemeanour.

## PERSONAL PRIVACY

Of interest to many observers is how the RIP Act (as 'amended' by the Regulations) fits in with, and indeed whether it is consistent with, the HRA and the DPA. The HRA came into force in the UK in October 2000. Although it is principally enforceable against Government bodies as opposed to corporate entities (the so called 'vertical effect'), it is widely thought that it may be relied upon against corporates or individuals via the 'back door' as other UK legislation is to be interpreted in accordance with it. How the Regulations are used by a company could, therefore, still be challenged if this is not in compliance with the HRA.

Specifically the HRA provides (amongst other things) for 'respect to correspondence, and gives individuals (and companies) the right to personal privacy. Monitoring of E-mails and other communications could easily be found to be inconsistent with this if taken too far. Similarly, in monitoring, employers may well have access to personal data (not just about their employees) which is subject to the requirements of the DPA.

The Data Protection Commissioner issued a draft Code of Practice<sup>3</sup> (the "Code") concerning the application of the DPA to the employer-employee relationship, back in October of last year. Unfortunately given the time that the draft Code was issued it did not take account of the Regulations (as it was prepared before the Regulations came into effect). It remains to be seen whether amendments will be made before the Code is finalized.

The draft Code deals with the application of data protection to employment generally. As such the issue of monitoring is only a part of it. Again I do not plan to detail its other provisions in this article. On the subject of monitoring the draft Code currently recognizes that the monitoring of communications per se does not necessarily give rise to data protection issue. This is only likely to happen when the interception or monitoring will actually give access to or involves the use of personal data.

Without seeking to water down in any way the basic requirements of the DPA, the draft Code attempts to set out some basic guidelines. Compliance with these guidelines will not necessarily ensure compliance with the DPA, but should go a long way towards doing so. The overriding principle behind the guidelines suggested by the draft Code is that any intrusion on an employee's privacy or autonomy should be in proportion to the benefits of the monitoring.

In particular the draft Code provides series of general considerations that businesses should take into account when considering monitoring. It then goes on to provide some specific guidance depending upon what sort of communications might be involved. There is insufficient room in this article to detail all the proposed provisions, as they run to several pages. However, they recommend, amongst other things, that businesses carry out the following as part of any actual or planned monitoring:

- establish the specific business purpose for which monitoring is to be introduced
- assess the impact on privacy/autonomy of staff
- consult with relevant trade unions or other employee representatives
- document both the business purpose and the impact assessment
- consider whether comparable benefits can be achieved using other methods
- make staff aware of the monitoring
- use personal data obtained only for the declared purposes

Some of this is no doubt common sense, particularly in industries such as financial services where monitoring is commonplace. However, they are probably unlikely to be followed elsewhere where monitoring is not regular e.g. to identify or obtain evidence of wrongdoing by particular members of staff.

Clearly any business intending to monitor or intercept employee communications is going to have to take into account both the DPA and the final Code of practice. The main difficulty it will face is working out in advance what precisely it will have to do, or not do, before it actually reads or hears the specific content.

The Government's intention, by introducing the RIP Act, was to strike the right balance between protecting the privacy of individuals and enabling industry and business to get the maximum benefit from new communications technology. In doing so the Government also hoped to comply with the HRA, the DPA and the Telecommunications Data Protection Directive.<sup>4</sup> Critics of the new legislation, however, argue that the RIP Act clearly contradicts both the HRA and the Code, highlighting the Government's confusion on the issue of monitoring. Even if this is not the case, any employer wishing to take advantage of these rights has to take of account (and in all likelihood seek specific advice on) not only the Regulations but also on what steps may be needed to ensure it remains compliant with the DPA and the HRA.

Only time will show the effectiveness of the RIP Act and whether it has succeeded getting the balance right. Hopefully, further guidance from the Data Protection Commissioner will shed some further light on this. However, in the meantime, businesses will need to be cautious if they intercept communications.

**Mark Crichard**, Partner, Technology Media & Communications Group, Garretts.

## FOOTNOTES

<sup>1</sup> Sections 1(1) and 1(2).

<sup>2</sup> Section 3(1).

<sup>3</sup> A copy of the draft Code of Practice can be obtained from the Data Protection Commissioner's website at <<http://www.dataprotection.gov.uk>>.

<sup>4</sup> Directive 97/66/EC of 15/12/1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.