Employee dismissal for computer misuse: obtaining the evidence

Bridget Treacy and **Purdey Castle** explain how employers can collect data for their investigations and stay within the law.

Misuse of an employer's data and computer systems is hardly a new issue, although T-Mobile's recent experience (p.21) of a rogue employee apparently selling thousands of its customer records has brought the issue firmly back into the spotlight. Where misuse of data and/or computer systems is suspected, the employer will wish to gather or preserve evidence of wrongdoing. This may involve gaining access to an employee's computer. In this article, we revisit the circumstances in which employers can gain access, and what safeguards they must be mindful of both to preserve the evidence and to ensure it may be used in legal proceedings.

The challenge

Malicious, negligent or merely careless employees pose a significant threat to the security of an organisation's information assets and may expose an organisation to the risk of contractual, civil and, in certain circumstances, criminal liability. There is a critical need to identify and mitigate these types of threats. Most employers have in place policies setting out the boundaries of acceptable computer and Internet use, but many such policies focus only on security issues or deal in generalities, rather than in specifics, which limits their value. These policies should be reinforced through the implementation of technical controls, training, general awareness raising and through clear lines of accountability within the organisation.

The existence of strong policies, good training and technical safeguards can minimise liability risks, but these risks cannot be completely eliminated. Determined employees will inevitably find a way to circumvent such controls. In the event that controls are circumvented, organisations may deal with the incident as a disciplinary matter, which may result in the dismissal of the employee for misconduct.

From an employment law perspective, it is important for an employer to set out in detail the rules relating to use of the organisation's computer systems. If disciplinary action is taken against an employee for misconduct (whether relating to computer misuse or otherwise), then it is for the employer to show that the dismissal was fair. The employer must be able to demonstrate that dismissal was a reasonable response (that is, not disproportionate) in all the circumstances. This means that the employer must be able to show that the dismissal was due to a genuine belief on reasonable grounds that the employee was guilty of the misconduct in question. Evidence of the employee's actions will be required. This evidence may consist of eye-witness accounts or, more commonly, include forensic evidence gathered from the employer's computer systems.

It is open to an employee to challenge how an employer has obtained information relied on in the context of disciplinary proceedings. Information that is obtained unlawfully and relied upon by the employer in disciplinary proceedings will almost certainly be challenged. Employers must proceed carefully when collecting evidence.

It is open to an employee to challenge how an employer has obtained information relied on in the context of disciplinary proceedings.

Gathering evidence lawfully

Large organisations invariably deploy automated monitoring to safeguard their systems. Many of these systems are sophisticated and configured to specific triggers that reflect the particular organisation's published security controls and employee acceptable-use guidelines. When an employee breaches those guidelines or controls, they trigger the monitoring software, capturing a record of the infringing use. Other systems routinely use key word searches to carry out automated scanning of email content and traffic, and monitor or block access to certain websites. Providing these automated systems are a proportionate response to risk, the basis of their use is made clear to employees, the systems are implemented in accordance with legal requirements and appropriately configured, and there are adequate safeguards to preserve the collected evidence, then it can be difficult to challenge the evidence.

In other circumstances where an employer suspects misconduct, the employer may wish to carry out targeted monitoring, including accessing emails sent and received by an employee. Where an employer suspects criminal activity or where the suspected misconduct is so serious that the employer is considering the dismissal of the employee, it is also becoming common for organisations to engage external computer forensic experts to assist with gathering evidence. In carrying out any and all of these activities, great care is required and an organisation must consider the requirements of the following legislation:

- the Human Rights Act 1998;
- the Data Protection Act 1998;

- the Regulation of Investigatory Powers Act 2000; and
- the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Human Rights Act 1998

Article 8 of the European Court of Human Rights (ECHR) creates a general right to privacy and is the right most likely to be cited by employees seeking to challenge any monitoring by an employer. Under Article 8, employees do have the right to some degree of privacy at work. In *Copland v UK* the ECHR ruled that the collection and storage of personal information relating to an employee's telephone, Internet and email usage amounted to an interference with the right to respect for private life under Article 8 (*PL&B UK*, July 2007, p.21). The Human Rights Act 1998 (HRA) incorporates most of the articles of the ECHR into UK law. Under the HRA:

- It is unlawful for "public authorities"[1] to act in a way that is incompatible with the HRA;
- Legislation implemented within the UK must be compatible with the rights incorporated by the ECHR; and
- UK courts and tribunals are required to interpret all legislation as far as possible to be consistent with the rights incorporated by the HRA.

The right to privacy under the HRA is not an absolute right. To justify any interference with this right any act which is incompatible with this principle must be in pursuit of a legitimate purpose. Such legitimate purpose includes the prevention of a crime or the protection of the rights and freedoms of others. An employer may balance an employee's right to privacy against its own interests or the interests of its other employees.

If an organisation is contemplating action which might infringe an employee's rights under the HRA (for example, accessing the employee's emails or otherwise monitoring the employee's activities in the workplace), it must have regard to the doctrine of proportionality by ensuring its objectives are sufficiently serious to justify limiting the right to privacy and that the method by which the monitoring will occur is no more than what is necessary to achieve the relevant objective.

Data Protection Act 1998

Accessing an employee's computer or emails or monitoring an employee's online activities will, of course, be governed by the Data Protection Act 1998 if it involves the processing of information from which a living individual can be identified. In conducting such investigations or monitoring activities, employers must comply with the DPA and, in particular, the requirements that the data are processed fairly and for a limited and legitimate purpose, that individuals are informed of the processing (unless this would defeat the purpose of the processing in a law enforcement context), that the processing is proportionate to the purposes for which the data are being processed, the data are kept secure and, if any data are transferred outside the EU, that there is adequate protection for the data transferred.

The Employment Practices Code and Supplementary Guidance (the Code) issued by the Information Commissioner is not new but it provides useful, pragmatic guidance on when and how organisations may monitor employees and gather evidence. A failure to comply with any particular recommendation in the Code does not automatically equate to a breach of the DPA, but the Information Commissioner expects organisations to comply with the Code. The Code is intended to be consistent with employers' obligations under related legislation, such as the HRA and the Regulation of Investigatory Powers Act 2000 (discussed below). The Code recommends that employers should use an impact assessment to determine whether specific monitoring can be justified.

Right to private life

Employees have a legitimate expectation that they can keep their personal lives private. An employer will usually justify the routine monitoring of its employees on the grounds that monitoring is necessary for the pursuit of its legitimate interests. Data collected as part of an employer's routine monitoring activities may legitimately be used by the employer for other purposes, for example in connection with the prevention or detection of a crime, but care must be taken as the DPA generally permits data to be used only for the purposes for which they are collected. There are limited exceptions to this, including in the context of crime detection or prevention. However, employers should be as transparent as possible about monitoring in the workplace and the purposes for which such information may be used, and it assists if those purposes include a reference to the investigation of breaches of the corporate code of ethics or other relevant policies. Usually information about the nature and extent of monitoring activities will be communicated in an IT acceptable-use policy.

> An employer must be able to account for the data source, the process by which the data are collected, and ensure the integrity and authenticity of the evidence.

Before implementing any systematic monitoring, or embarking on targeted monitoring or forensic investigation, an employer must ensure it has in place detailed procedures and practices for dealing with the data collected as part of the monitoring activity. This data should only be kept for as long as is necessary for the purposes for which it was collected. For example, the data collected from systematic monitoring should be deleted after a very short period of time if it does not trigger any of the organisation's controls. Where data is used in connection with disciplinary procedures, it will need to be held for longer but should be destroyed after a reasonable period of time has elapsed following the completion of such proceedings (or once the risk of

proceedings no longer exists). Access to such information should be limited. For example, where systematic monitoring takes place, typically access to such information will be limited to the IT department. However, during an investigation additional access may be required by an organisation's legal department, HR managers and other senior personnel.

Where an organisation engages a third party to provide monitoring or computer forensic services, the organisation will need to ensure that it obtains appropriate guarantees from the third party regarding the security of the data, including in relation to any data transfers, and in relation to the purposes for which such data may be used. Detailed data protection clauses should be included in the contract. In proceedings an employer must be able to account for the data source, the process by which the data are collected, and ensure the integrity and authenticity of the evidence. The employer will therefore need to ensure that the nature of the processing carried out by the forensic expert is appropriate in the circumstances.

Regulation of Investigatory Powers Act 2000

An employer will need to ensure that any monitoring of employees in the workplace complies with the Regulation of Investigatory Powers Act 2000 (RIPA), which makes it unlawful in the UK to intercept a communication in the course of its transmission. Monitoring will be regulated by RIPA if it involves the "interception of a communication in the course of transmission". "Interception" occurs where some or all of the contents of a communication are accessed by or made available to a third party (that is, other than the sender or recipient) during transmission. Communication is defined broadly and includes most people or system-based communications. Examples of the types of monitoring systems that will be caught by RIPA include the recording of telephone conversations and systems which block e-mails, although simply opening an email that has already been opened by the intended recipient will not amount to interception under RIPA.

Communications can lawfully be intercepted under RIPA by:

(i) obtaining a court order; or
(ii) obtaining the consent of the individuals concerned.

Where consent is relied on, the interception will be lawful where the interceptor has reasonable grounds for believing that both the sender and the recipient have consented to the interception. It may be possible for an employer to obtain employees' consent to the interception of internal e-mails and telephone calls for certain purposes, but relying on consent is generally problematic where the sender or recipient are external to the organisation. To lawfully intercept its employees' communications, an employer will invariably rely on the grounds set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

LBP Regulations 2000

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations) permit the interception of communications without consent in certain circumstances. These include interception for the purpose of establishing the existence of facts, to ascertain compliance with regulatory or self-regulatory practices that apply to the business, or to determine or demonstrate the standards that are (or ought to be) achieved by those who use the organisation's systems in the course of their duties. Further, monitoring may be carried out for the purpose of preventing or detecting crime or for the purpose of detecting the unauthorised use of the system.

The right to intercept communications is restricted by the requirement that the interception must be effected solely for the purpose of monitoring communications relevant to the business. Personal communications may be accessed if it is necessary to gain access for business purposes, for example, when an employee is on holiday, but emails that are clearly personal from their heading, even where they are sent "in the course of business" may not be opened without further justification. To rely on the interception grounds in the LBP Regulations an employer must also have made reasonable efforts to notify its employees that interception may take place.

Maximise your ability to collect and use evidence

In the UK, an employer has greater rights than in many other EU jurisdictions to monitor system use and to collect evidence of an employee's online activities and email communications. Nevertheless, unless those rights are exercised carefully, and adequate safeguards taken, an employer may find that crucial evidence cannot be used in disciplinary proceedings against an employee. Key compliance considerations are set out below:

- Ensure there is a comprehensive policy describing the acceptable use of the corporate IT systems.
- Provide employees with training on the acceptable use policy during induction and periodically throughout their employment.
- Have in place a clear structure and policy for managing the use of monitoring tools and access to data gathered as part of any investigation. Ensure employees are told how, when and why they may be monitored.
- Implement an incident response programme to deal with the need to capture evidence at short notice. Ensure senior staff is involved in any decisions to undertake covert monitoring, which is only rarely justified. Maintain an audit trail of the decision.

AUTHORS

Bridget Treacy, Partner, and Purdey Castle, Associate, at law firm Hunton & Williams, London.
Email: btreacy@hunton.com and pcastle@hunton.com.

REFERENCES

1. There is no definition of "public authority" for the purposes of the HRA, but broadly a public authority includes a court or tribunal or any person who provides functions of a public nature.