



Email Risks for the Public Sector

This paper considers some of the main risks that public sector bodies face in the operational use of email. It also considers the legality of email monitoring and the role of an Acceptable Use Policy in monitoring strategy

Written for MessageLabs by Tamzin Matthew of Blake Laphorn Tarlo Lyons Solicitors

Table of Contents

How Liability Arises	3
The Risks	4
Obscenity	5
Defamation	6
Third Party IPR Infringement	6
Data Protection	7
Contract Formation	7
Confidentiality	7
Dealing with the Risks	8
Monitoring	8
The Role of the Acceptable Use Policy	9
Maximising Effectiveness of the AUP	9
Summary	10

The Public Sector in the Electronic Age

In recent times there has been an unprecedented effort to bring public services into the electronic age. In line with EU directives, the UK government launched the Electronic Government programme, with the intention that all government services to citizens would be delivered by cheap, efficient and convenient electronic means. Similar programmes have been initiated in other public sector bodies.

Clearly we now work in an age where e-mail and Internet access is critical to the public sector. The ease of use and scale of information that can be obtained or distributed by e-mail and the Internet makes these tools invaluable. However, the same attributes can also cause severe difficulties to public sector organisations. Although they are not driven by profit considerations, they operate on strict budgets in a political environment, where they are obliged to protect public money and property and have a reputation to preserve. In many respects they are expected to set an example.

In late 2007 the Observer newspaper made requests under the Freedom of Information Act to 65 public sector bodies and discovered that e-mail and Internet misuse was rife in the public sector. It discovered that over the previous three years, the public sector bodies it questioned had disciplined a total of 1722 people for IT abuse, and had sacked 130. E-mail abuse is a problem that is only likely to increase as more public sector users come online.

This paper considers some of the main risks that public sector bodies face in the operational use of e-mail. It also considers the legality of e-mail monitoring and how Acceptable Use Policies should be used in the context of a monitoring strategy. It is only designed as an outline guide to the issues, and detailed legal advice should always be sought in specific situations. It is also an independent view of the issues, as Blake Lapthorn Tarlo Lyons does not endorse the products of MessageLabs or of any particular vendor.

Organisations can be criminally liable for e-mail facilitated acts that are committed due to the neglect of its officers.

How Liability Arises

The starting point is a consideration of how a public sector body may become liable for the acts of the users of its e-mail systems. This principle of liability for the acts of others is called "vicarious liability".

Firstly, public sector employers will generally be held responsible for the acts of their employees committed in the course of their employment, even if those acts were expressly forbidden to the employee. It is often difficult to predict whether an act will be found to be in the course of employment because the authorities are sometimes conflicting, but this in itself should be a warning to employers that they should be prepared for the possibility that they may be vicariously liable in circumstances that may not be immediately obvious. For example, In Chief Constable of the Lincolnshire Police v Stubbs¹, a male police officer subjected a female colleague to several incidents of inappropriate sexual behaviour at social gatherings immediately after work. The Employment Appeal Tribunal found that despite the fact that the gatherings were not in the workplace or organised by the employer, Lincolnshire Police was vicariously liable for unlawful sex discrimination.

Public sector organisations may also be vicariously liable for the acts of their agents, such as temporary staff when those agents are acting, or appear to be acting within the scope of their authority. Again, it does not matter that the wrongful acts were prohibited. For example, local

¹ [1999] IRLR 81 EAT.

authorities may be liable for the acts of their councillors committed when acting on behalf of the local authority.

Other sources of liability may arise where a public sector body becomes aware of wrongful acts committed on its system, but fails to do anything about them. For example, if third parties are sending racist e-mails into the employer's system and the employer does nothing to prevent their occurrence, recent developments in the law suggest that it could be liable for a discrimination case (e.g *Gravell v Bexley Council*²). In some statutes, organisations can be criminally liable for e-mail facilitated acts that are committed due to the neglect of its officers.

The Risks

Harassment

There are certain terms that are implied into an employment relationship, no matter what the written employment contract may say. In the case of *Wigan Borough Council v Davies*³, the courts stated that it is an implied term that the employer:

“will render reasonable support to an employee to ensure that the employee can carry out the duties of his job without harassment and disruption by fellow workers”.

This statement has been approved in subsequent cases. The employer also has a duty to provide a secure, safe and healthy working environment which may be breached if an employee becomes unwell as a result of the harassment.

Employees can sue their employers directly in the courts for harassment carried out by fellow workers.

Harassment need not take the form of a targeted campaign of offensive e-mails. It may occur as a result of the victim being exposed to offensive content that has been circulated generally, or even where the victim has not been the direct recipient of offensive e-mails, but has been exposed to an environment where such content has been viewed by colleagues in a general “atmosphere of obscenity”⁴. When harassment occurs an employee may consider that the offence or distress that they experience, or the effect that the harassment has, is such that the employer has breached the implied duties in the employment contract, and therefore the employee is entitled to treat the contract of employment as being at an end as if he had been unfairly dismissed, and to claim damages for the breach. This is called constructive dismissal.

The maximum damages that can be awarded in a constructive dismissal case that does not have an element of discrimination in it is £69,900.⁵ However, where the harassment has an element to it that suggests that it amounts to discrimination under various pieces of legislation such as the Race Relations Act 1976, the Sexual Discrimination Act 1975 or the Disability Discrimination Act 1995, then the damages that can be obtained are unlimited. In each case the employer will not be liable unless he knows or ought to know about the harassment, and has failed to take reasonable steps to prevent it. E-mail monitoring, a clear Acceptable Use Policy and adequate training are likely to be considered to be “reasonable steps” that will provide a defence.

A new development that will be of concern to employers is that the Protection from Harassment Act 1997 can now be used directly against an employer. In a ground-breaking case in 2006 of *Majrowski v Guys and St*

² UKEAT/0587/06/CEA

(www.employmentappeals.gov.uk/Public/Upload/06_0587fhAMCEA.doc).

³ [1979] IRLR 127.

⁴ *Morse v Future Reality Ltd* (1996).

⁵ Employment Rights Act 1996, Section 124(1).

Thomas' NHS Trust⁶ the House of Lords confirmed that employees can sue their employers directly in the courts for harassment carried out by fellow workers. The advantages of using this route rather than the Employment Tribunal is that cases can be brought up to six years after the date of the offence, (whereas the time limit in the Employment Tribunal is 3 months, extended to 6 months if the grievance is lodged within the 6 months), and that there are no defences to a claim provided that the harassment occurred in the course of the harasser's employment. For a claim of unwanted harassment to be shown, the harasser must have engaged in unwanted conduct which has "the purpose or effect of

- a) violating the other person's dignity; or
- b) creating an intimidating, hostile, degrading, humiliating, or offensive environment; on the grounds of sex, gender reassignment, race, religion or belief, disability, sexual orientation or age".⁷

Clearly the unwanted conduct could be carried out by e-mail and so public sector employers should be careful to prevent harassment by whatever means possible.

Obscenity

Despite many highly publicised cases, employees persist in accessing inappropriate material, such as pornography, through work PC's. Public sector employees are frequently in the news for this kind of wrongdoing. In 2005, the Audit Commission undertook a survey of 400 public sector organisations, including local authorities, NHS trusts and police forces.⁸ It found that the accessing of pornographic and other inappropriate material at work made up around 47% of the computer misuse reported.

The storage of and publication by e-mail of material that is likely to "deprave and corrupt"⁹ may constitute a criminal offence under the Obscene Publications Acts. A prosecution is unlikely unless the employer is somehow colluding in the publication; however, the potential for such information to cause harassment, and the general damage to reputation that the circulation of such material can cause, means that public sector bodies should monitor for obscene material and make it clear in their Acceptable Use Policies that such material is unacceptable.

In the case of *Parr v Derwentside District Council*,¹⁰ Mr Parr was a Council official who viewed porn at work. The Council sacked him and he then claimed unfair dismissal, stating that he had happened on the images by chance. However, the Newcastle Employment Tribunal rejected Parr's claim for unfair dismissal and accepted that the fact that he was a public servant and a senior officer made the offence more serious than it might otherwise have been.

Downloading, circulating and viewing child porn is altogether more serious as an offence. The Protection of Children Act 1978 makes it illegal to make indecent images of children, and show them,¹¹ the Criminal Justice Act 1988 created the offence of mere possession of an indecent image of a child,¹² and the Criminal Justice and Public Order Act 1994 confirmed that pseudo photographs (computer generated images or those that alter

⁶ [2006] UKHL 34.

⁷ Regulation 5(1), Employment Equality (Sexual Orientation) Regulations 2003.

⁸ http://www.audit-commission.gov.uk/Products/NATIONAL-REPORT/2F4CC95D-4BC6-4e40-89FA-829C9D73438D/ICT_fraud_and_abuse_2004.pdf

⁹ Section 1, Obscene Publications Act 1959.

¹⁰ Unreported.

¹¹ Section 1, Protection of Children Act 1978.

¹² Section 160.

Despite many highly publicised cases, employees persist in accessing inappropriate material.

The Freedom of Information Act, which requires public sector bodies to disclose recorded information, may lead to the discovery of libellous e-mails

images of adults to look like children) would count as indecent images of children under the other legislation.¹³

Downloading or e-mailing child porn is deemed to be making an image or showing it, and organisations will be liable for a corporate criminal offence under the Protection of Children Act if the crime occurred with the consent or connivance of, or was attributable to the neglect on the part of any director, manager, secretary or other officer of the body, or any person who was purporting to act in such capacity.¹⁴ The officer or other person listed above will also be personally liable, as well as the employee who committed the offence. Apart from the reputational damage, public sector bodies need to be vigilant to prevent themselves being found to be negligent, and should deal with issues swiftly.

In 2004 the Department for Work and Pensions cracked down on the activities of civil servants, and disciplined over 200 staff. One particular staff member was charged with 32 counts of possessing child pornography.

Defamation

A defamatory statement is an untrue statement that tends to lower the reputation of an individual or organisation in the minds of right thinking individuals. An organisation can be exposed to liability for defamatory statements published by e-mail, notwithstanding that the e-mail may never leave the organisation.

The provisions of the Freedom of Information Act, which requires public sector bodies to disclose recorded information, may lead to the discovery of libellous e-mails than might previously have been made public. Those libelled can sue for damages and seek an injunction to prevent further publications. Most people are aware of the case involving Norwich Union, where Norwich Union paid out £450,000 in damages to a company that had been defamed by Norwich Union employees who circulated e-mails wrongly alleging that the claimant was experiencing financial difficulties.

In the highly political world of the public sector organisation, it is easy to see how defamatory conversations in relation to particular individuals or supplier organisations might circulate via e-mail.

Third Party IPR Infringement

Copyright protects documents and works such as software and sound recordings, that are original (in the sense of not being copied), where effort has been invested in their creation. Copyright protects the economic value in that investment of effort. It is a breach of copyright, not only to copy copyright works without the permission of the copyright holder, but also to issue copies to the public, or show or play them to the public.

A new development in the public sector has been the implementation of the Re-use of Public Sector Information Regulations 2005. These Regulations were designed to encourage public sector bodies to generate income from the information they hold, by licensing that information to third parties. This information will often reside in copyright works, and the copyright will be owned by the relevant public sector body. E-mail often provides a quick and easy route for unlawful and unauthorised disclosure and circulation of copyright items.

Unauthorised or unthinking disclosure of the public body's own copyright works will obviously deprive the public sector owner of the revenue that would otherwise have been generated from the licensing of that information. Such disclosure may also expose the public body to liability, as the Re-use

¹³ Section 84.

¹⁴ Section 103, Children Act 1989.

E-mail often provides a quick and easy route for unlawful and unauthorised disclosure and circulation of copyright items.

of Public Sector Information Regulations require public bodies to ensure that if certain information is licensed to one party, all other interested parties are granted a licence on similar terms (unless an exclusive arrangement is in the public interest).¹⁵ An unauthorised disclosure of a copyright work to a third party may be considered to be a breach of these terms.

The position is probably more catastrophic in relation to the disclosure of the copyright works of third parties. The act of disclosure and circulation by e-mail will usually involve both copying and issuing and showing copyright works to the public. If system users breach copyright in the copyright works of others, the copyright holder can then launch an action for damages against the disclosing organisation, which will result in expensive litigation and damaging publicity.

Data Protection

Most public sector organisations are data controllers under the Data Protection Act 1998. A data controller is the organisation that controls the manner in which and the purposes for which personal data is processed. The data controller is responsible for compliance with, and primarily liable for breaches of the Data Protection Act. The data controller has to take appropriate organisational and technical measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Part of compliance with principle 7¹⁶ will involve measures to prevent unauthorised or unlawful processing by e-mail, and any unauthorised disclosure of personal information by e-mail, will potentially be a breach of the Act, which gives rise to the right of affected individuals to sue for loss and may provoke enforcement action by the Information Commissioner. As the Child Benefit Agency and the DVLA have recently discovered, such breaches of the Data Protection Act can lead to damaging publicity, and even dismissals.¹⁷

Contract Formation

Organisations are often under the misapprehension that, for a contract to be legally binding, formal requirements or procedures need to be met or followed. In fact, a binding contract need not even be in writing. An exchange of promises by e-mail in the work environment can create a binding contract, or vary an existing one. Public sector organisations are particularly at risk when dealing with suppliers, where an e-mail could signify acceptance of highly prejudicial terms, or simply to terms that the person sending the e-mail has not really accepted. In *Hall v Cognos Limited*,¹⁸ an ill thought-out e-mail from a manager was found to vary a written company expense policy, to the employer's expense.

Confidentiality

E-mail can be used as a silent tool to send confidential data out of a public sector organisation. This may occur through the actions of a disgruntled employee, or through the actions of someone wishing to help their associates gain an advantage – perhaps in a supplier selection process. It may also occur simply through ignorance or a lack of thought. This can be highly damaging to a public sector organisation. Despite the fact that public sector bodies are required by the Freedom of Information Act to disclose their recorded information, sensitive information and information received

¹⁵ Section 14, The Re-use of Public Sector Information Regulations 2005.

¹⁶ Schedule 1, part 1, Data Protection Act 1988.

¹⁷ http://www.ombudsman.org.uk/improving_services/selected_cases/PCA/sc0103/c1513.html

¹⁸ (unreported, 17 February 1998).

under an obligation of confidence is usually protected by exemptions; a breach of confidentiality can be just as devastating to a public sector body as it would be to a private sector organisation. Public sector organisations may be vicariously liable for breaches of confidentiality caused by their employees and agents, but they may also be liable contractually if the disclosure arises from a failure to follow agreed security measures.

Dealing with the Risks

Monitoring

There are three main pieces of legislation that are relevant to lawful e-mail monitoring:

The Regulation of Investigatory Powers Act 2000 created the offence of unlawful interception on a private network.¹⁹ This allows those who suffer loss as the result of an unlawful interception by a public body on its own system, to sue for damages.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("Lawful Business Regulations") allow monitoring for a number of "business" purposes (which includes the business of a public authority).²⁰ Permissible purposes include establishing whether a communication is private or work-related, investigating unauthorised use of the system and ensuring the effective operation of the system. The system owner must make "all reasonable efforts" to inform system users (including those sending information in from external systems) that communications may be intercepted, or the Regulations cannot be relied upon.²¹ Note also that if the system is not intended for predominantly work use, the Regulations cannot be relied upon either. This may affect the way that some organisations may police their systems.

Public bodies are subject to the Human Rights Act 1998, which provides that everyone has the right to the privacy of his correspondence and a private life.²² This right can be infringed, and private correspondence monitored, provided that the infringement is sanctioned by law, necessary in a democratic society and is proportionate given the harm that is protected against. Claims under the Human Rights Act can be made directly against public sector bodies.

In practice public sector bodies should assess and document the threats they are trying to protect against in order to show the monitoring is only sufficiently intrusive to secure that protection. This may assist in mounting a defence to a claim from a system user. Public bodies can be robust in telling their staff that there can be no expectation of privacy if the business system is used for private e-mail. However, notwithstanding this, if an e-mail is clearly private, or an e-mail that is not marked turns out to be private, the privacy of the individual should still be respected unless there are good reasons not to.

Public sector bodies should use automated monitoring wherever possible as this is less intrusive to the employee. Public bodies may also have to consult with unions when finalising their policies.

E-mails contain personal data so e-mail monitoring is processing of personal data and governed by Data Protection Act 1998. The monitoring must therefore be undertaken in accordance with the eight data protection principles. One of the main requirements of the principles is that those individuals whose personal data will be processed must be told of the

¹⁹ Section 1.

²⁰ Section 3.

²¹ Section 3 (2) (c).

²² Schedule 1, Article 8.

Public sector bodies should use automated monitoring wherever possible as this is less intrusive to the employee.

processing and their explicit consent obtained, as it is possible that sensitive personal data may be processed.²³

The Role of the Acceptable Use Policy

Usually system owners give the information necessary to comply with the Lawful Business Regulations and the Data Protection Act in one Acceptable Use Policy (AUP). This document is key, as its other main function is to outline to employees what disciplinary action may be taken if the policy is breached.

Maximising Effectiveness of the AUP

1. Compliance with the Acceptable Use Policy should be an express term of the employment contract, temporary services contract or other contract governing the relationship between the user and the public body. This makes it easier to show in serious cases that a breach of the Acceptable Use Policy is a breach of the employment or other contract, which therefore entitles the public body to terminate the relationship.
2. The Acceptable Use Policy should also make it clear which activities will be in breach of the policy and what penalties will be levied for failure to comply. If possible some indication should be given as to which activities will be considered to be gross misconduct leading to dismissal, and which will merely disciplinary issues. An employee succeeded in a claim of unfair dismissal against the Royal Bank of Scotland (*Goudie v Royal Bank of Scotland plc*²⁴) after his employment was terminated for a breach of the bank's Acceptable Use Policy. It was held that the bank's failure to explain to the employee, as part of the disciplinary process, how the bank "graded" the offensive nature of the material involved and what sanctions would apply to each grade, rendered the dismissal unfair.
3. A regular review of the policy should ensure that new threats are dealt with as and when they arise. Public bodies should ensure that changes are properly notified to users, and that users receive training when necessary.
4. The public sector body should have proof that the policy has been read and understood, both when first giving access to the system and when making changes to the policy. If employees and other users are required to sign the policy, then the public body has the added benefit of evidence that the user has seen the policy. A signature block that states that by signing the policy the user is indicating that he or she has read and understood the policy will add to the weight of evidence. Ideally it should be a condition of access to IT systems that the policy has been signed.
5. Inconsistent enforcement increases the likelihood of a case for racial or sexual discrimination. In *Meek v London Borough of Hillingdon*,²⁵ a white male claimed that his dismissal for circulating pornographic e-mails constituted sexual and racial discrimination because a black female who was also involved was not sacked.

Public sector bodies should be conducting e-mail monitoring to minimise this risk.

²³ Schedule 2, section 1.

²⁴ [2004] All ER (D) 33 (Jan).

²⁵ EAT/0422/03 DA.

Summary

The liability of public bodies for misuse of their e-mail systems arises from several quarters. The risk that this liability presents is not insignificant, and public sector bodies should be conducting e-mail monitoring to minimise this risk. The monitoring must be undertaken in accordance with the protections for users' privacy that are laid down in legislation, and the details of the monitoring policy should be contained in a clear Acceptable Use Policy covering use of e-mail and the web. This policy must be enforced consistently, or discrimination claims may arise.

Gail Becker, Group Product Manager at security specialists MessageLabs explains how MessageLabs Email Security Services can address the concerns around the operational use of email within the Public Sector:

'For Public Sector customers, MessageLabs provides a suite of email services which can be used to monitor email use and provide controls so email communications can be used safely and productively, in line with policy.'

'Our Content Control service scans all inbound and outbound emails, offering an unmatched capability in blocking emails containing unauthorised or inappropriate textual content. With our Email Image Control Service obscene images contained in emails can be prevented from entering or leaving your network; where IP or other sensitive information needs the utmost confidentiality our Boundary Encryption service will ensure all email communications in and out of your organisation are securely encrypted with TLS.'

For more information visit www.messagelabs.co.uk/products/email

www.messagelabs.co.uk
info@messagelabs.com

Freephone UK
0800 917 7733

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
FeringasträÙe 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

© MessageLabs 2007
All rights reserved

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300