



MessageLabs[®]

Be certain

Email Archiving UK law, regulations and implications for business

A White Paper written for MessageLabs by Tamzin Matthew of Blake
Laphorn Tarlo Lyons Solicitors

Table of Contents

About the Author	3
Overview	3
Freedom of Information Act	3
The Data Protection Act	4
The Employment Tribunal	5
Court Actions	5
The Sarbanes-Oxley Act	6
Industry-specific Regulations	6
Summary	7

About the Author

Tamzin Matthew is a partner specialising in IT and information security at leading South East firm, Blake Lapthorn Tarlo Lyons. The firm is consistently in the top tier for IT law in the South East in the Legal 500. Tamzin is Secure Computing Magazine's expert legal columnist. Neither Tamzin nor her firm endorse any particular product or vendor, and MessageLabs commissioned Tamzin to write the legal piece in this white paper as an objective and independent assessment of the legal issues surrounding email archiving.

Overview

Many information managers have concluded that basic, usually folder-based search-and-retrieval functions in their email applications are simply not enough to rise to the challenge, and a state-of-the-art-email storage facility with enhanced retrieval and management capabilities is the only viable solution.

The use of business email has grown exponentially over a relatively short period of time, bringing with it the huge advantages of worldwide, cost-effective, easy and near-instantaneous communication. But as all those involved in the management of IT systems know, the growth in email usage has brought its own challenges.

The concept of information governance is not a new one, but the challenge posed by the sheer volume of information generated by email is. Even organisations with well-defined and well-enforced policies on the use of traditional communications have struggled to police electronic communications. The sharing of internal information is a key challenge for many large organisations, and unless information can be easily located and retrieved, an organisation risks confusion, duplication of effort, and embarrassment. On top of these costly irritations, the same organisation may also suffer more serious losses resulting from an inability to take action against wrongdoers, and an inability to defend itself adequately against legal actions, some of which may be based on questionable evidence. Equally importantly, the law is beginning to adapt to deal with the rolling back of the electronic frontiers. Where organisations are not willing to take electronic data management seriously, recent legal developments are likely to compel them to take notice.

Freedom of Information Act

Those working in the public sector have experienced perhaps the most dramatic legislative change to affect email management in recent years. The Freedom of Information Act 2000 ("FOIA") came into force on 1st January 2005 and gave the public new rights of access to recorded information held by public authorities. Email communications fall within the definition of "recorded information". Anyone, anywhere, without giving either proof of identity or details of their motive for making a request, can ask for a copy of an email. The deadline for responding is 20 working days from the date of receipt of the request, and many public authorities have discovered that their current facilities for searching and retrieving archived emails have caused considerable difficulties in meeting the deadline. A search of the Information Commissioner's decision notices (which can be found at www.informationcommissioner.gov.uk) shows that the majority of public authorities that are named have earned their place in this dubious hall of fame for this very reason.

One of the most shocking aspects of the FOIA is the fact that it is retrospective. Public authorities are obliged to provide information in emails that were generated before the date the FOIA came into force, forcing them to search through archives. In a recent case in the Information Tribunal, (where decisions by the Information Commissioner are reconsidered when those concerned do not agree with his decisions), it was clearly stated that if a document is at all recoverable (for example, a trace of it remains on the network) it must be retrieved in order to comply with the FOIA. Many of those charged with information governance have concluded that basic, usually folder based search-and-retrieval functions in their email applications are simply not enough to rise to the challenge, and that a state-of-the-art-email storage facility with enhanced retrieval and management capabilities is the only viable solution.

State-of-the-art-email storage facility with enhanced retrieval and management capabilities is the only viable solution.

Public authorities are also having to wake up to the fact that an ability to locate, assess and delete redundant material is as important as an ability to preserve the more relevant content.

Whilst deletion of redundant material is essential, the Freedom of Information Act also imposes criminal sanctions where the deletion is for more sinister reasons. Section 77 of the FOIA makes it a criminal offence to alter, deface, erase, destroy or conceal any record, including an email, with the intention of preventing disclosure by a public authority. This criminal penalty can be imposed on the individuals concerned, and this personal liability can fall upon employees and officers of an organisation, or consultants and other temporary staff. Clearly, a system with the built-in ability to protect system integrity and to provide a reliable audit trail could provide vital evidence to protect a public authority from liability where the wrongdoing is committed by an individual acting for his or her own ends.

Public Authorities are also expected to comply with a statutory code on records management that has been issued under the FOIA, (called the s46 Code). Very early on in the history of the FOIA it was anticipated that records management (or rather a lack of it) would be a major hurdle for compliance with the new right to public information. The Code requires all public bodies to treat the records management function "as a specific corporate programme". The Code emphasises that electronic records, such as emails, should be managed with the same care accorded to manual records, and that the records management programme, "should bring together responsibilities for records in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal." The National Archives has issued useful guidance on developing a policy for managing email, in support of this requirement for good records management. The guidance recommends that archiving and records management should be considered alongside the more usual elements of an Acceptable Use Policy. Clearly, an archiving facility that allows the organisation to set the archiving functions to run in accordance with the terms of its own policy will give that organisation a significant foundation from which to operate.

The Data Protection Act

The recent developments under the Freedom of Information Act have revolutionised the public sector's approach to the management and storage of electronic mail and have grabbed a large quota of the headlines. However, the Data Protection Act 1998 ("DPA") applies to the private and public sector alike and continues to create headaches for those with poor data management facilities.

The DPA gives individuals the right, on producing evidence of their identity, to have a copy of personal data held about them. Personal data covers information that relates to a living individual from which that individual can be recognised, where that information is processed automatically as part of an electronic mail system, as well as manually and in other automatic processing contexts. Without the ability to retrieve reliable information, and an accurate audit trail, an employer will be exposing itself to unnecessary risks.

The definition of "personal data" changed in 2005, due to the decision in a case called *Durant v. Financial Services Authority*, in which it was decided that for information from which an individual can be recognised to be personal data, an additional requirement is that the information has to be focused on the individual, biographical in some significant sense, and likely to have an adverse effect on the privacy of that individual. Post *Durant*, legally speaking not all email communications are now considered to contain personal data. Previously, the mere mention of a person in an email was likely to mean that the information in that email would have to be disclosed. However, in 2007, guidance was issued by the Information Commissioner that suggests that notwithstanding the *Durant* case, as a matter of good practice organizations should take a wide view on the definition of personal data, and treat all information that relates to an identifiable living individual as personal data. In practice whichever view is taken, the task of retrieving personal data that is requested by an individual under the DPA can be onerous.

All this activity must be completed within a 40-day time limit for compliance which runs from the date that the request and the fee have been received and the retrieved information must be assessed to remove third party data and other information that should not be disclosed. Organisations recovering personal data from email records are only entitled to charge £10. Although regulations under the

Without the ability to retrieve reliable information, and an accurate audit trail, an employer will be exposing itself to unnecessary risks

FOIA introduced the right to charge more for retrieving information under the DPA, this right to charge only applies to unstructured manual information held by public authorities. Clearly there is a cost benefit in ensuring that requested emails are retrieved as quickly and easily as possible.

The DPA also requires organisations to take appropriate technical and organisational measures to prevent unauthorized or unlawful processing of personal data, and against accidental loss or destruction of personal data. In the context of email management, this means that access to any email system and related storage device should be controlled, whether that access comes from within or outside an organisation. What is "appropriate" depends on the state of technology at the time that the requirement is being considered, and the costs of that technology in relation to the likely threat to the individuals whose data may be processed. An average workplace email system is likely to contain a large amount of personal data, some of which will be sensitive and therefore require a higher standard of security than other types of data. For example, the system may contain highly confidential details of an employee's health, or details of action to be taken against an employee for criminal wrongdoing. An encrypted, secure archive is likely to fulfil this requirement with ease, and provide an essential backup should the main system fail in some way which leads to loss of personal data.

The Employment Tribunal

As anyone involved in IT security will know, some of the greatest threats for an organisation come from within. Email misuse is an ever-present threat, which needs to be managed carefully, and in many cases email will provide evidence of other types of wrongdoing. As many employers will know to their cost, employees are well protected under law, and the employer needs to be sure of its grounds before making a dismissal. Without the ability to retrieve reliable information from emails, and an accurate audit trail, an employer will be exposing itself to unnecessary risks.

In some cases there will be insufficient evidence to justify action against an employee who is clearly not behaving in the interests of the employer; in others, the fairness of a dismissal made on suspect evidence will be challenged in an Employment Tribunal. The highest possible award in an Employment Tribunal for unfair dismissal claims is currently £69,900. However, if a dismissal is made without sufficient evidence for that dismissal, an employee may claim that the dismissal was founded on discriminatory grounds, such as race or sex, which entitles an employee to unlimited damages (plus a possible additional award of damages for injury to feelings of up to £25,000). It should also be noted that only in very unusual circumstances will an employer be able to recover its legal costs if it is successful in an Employment Tribunal.

In relation to disciplinary action, an inability to take decisive action under an Acceptable Use Policy, or to detect wrongdoing, based on poor records management, will weaken the ability of the employer to enforce that policy when it needs to. If there is a hit-and-miss approach to enforcement, it is far easier for a sacked employee to allege that he or she has been unfairly treated because previous offenders have escaped with lesser penalties.

The evidence obtained from an insecure and unreliable system that is not governed by clearly documented and enforced rules will be open to dispute and questioning by the opponent.

Court Actions

A similar risk is present in relation to court proceedings. In most cases, a wronged party has six years from the date that a contract has been breached or a civil wrong committed to bring a court action.

Even when a court action is taken promptly, a case may not come to court until several years after the event, and memories of the exact events will be hazy, or those involved may be unwilling, or unavailable as witnesses. Often the only clear, contemporary evidence will be contained in emails. Conversely, an organisation may need email evidence to launch its own action to protect its position. A party in a dispute may have a significant advantage over its rival if it can retrieve the evidence faster and at a lesser cost than the rival. The lack of readily available evidence may lead to a settlement of a dispute that might otherwise have been successfully fought and won. Court disclosure rules make it clear that even where an email has been

Evidence obtained from an insecure and unreliable system that is not governed by clearly documented and enforced rules will be open to dispute and questioning by the opponent.

Failure to have the best-possible archiving system and procedures could mean the difference between winning and losing an important case

deleted, if it is reasonably possible to retrieve it, it should be retrieved. An additional point to note is the weight that can be attached to favourable evidence is based on the reliability of that evidence. The evidence obtained from an insecure and unreliable system that is not governed by clearly documented and enforced rules will be open to dispute and questioning by the opponent.

Where an organisation can show by production of supporting evidence that the system in which the email evidence was held is secure and separate from the main system, that there is an audit trail, and that the policy in relation to archiving is consistently applied, that organisation has the best chance of its evidence being believed. Where it can be shown that the policy is consistently applied because the system operates in accordance with policy rules, rather than human compliance, the weight of the evidence can be even greater.

Failure to have the best possible archiving system and procedures could mean the difference between winning and losing an important case. Given the expense of fighting court actions, this is something where organisations should look to manage away the risk.

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act is a piece of US legislation that regulates financial reporting. Passed in the wake of the Enron episode and several other notable financial scandals in the US that involved suspect financial reporting, the Act was designed to revive investor confidence by compelling US companies to produce accurate and transparent financial information. Any company with a listing on NASDAQ or the New York Stock Exchange has to comply with the Sarbanes-Oxley Act, even if it is a European company with headquarters outside the US. UK subsidiaries of US corporations are usually required to ensure that the transactional data that they hold and share with their US parent will meet the requirements of the Act.

Section 404 of the Sarbanes-Oxley Act requires all annual financial reports to include a statement attesting that a company's management has implemented an adequate internal control structure over financial reporting, and requires that statement to include an assessment of the effectiveness of the control structure. Any failures in that system of controls must also be reported.

The internal control structure that section 404 refers to is defined as including measures to ensure that records are maintained in a way that accurately and fairly reflects financial transactions in reasonable detail. Those records must be adequate enough to permit preparation of financial statements in accordance with applicable regulations. The structure should also include controls that will prevent or quickly detect unauthorised use of the company's assets that could have a material effect on a company's financial statements. These provisions apply as equally to records contained in email communications as to any other form of communication. Companies will need to ensure evidence of their financial transactions contained in emails is properly preserved and are capable of being retrieved. Checks will also have to be in place to ensure that email communications are properly monitored to enable the prevention or detection of any unauthorised transactions.

Industry-specific Regulations

Organisations will also need to pay specific attention to the regulations governing the vertical industries in which they operate. For example the Financial Services Authority (FSA) is the independent body that manages the regulation of financial services providers in the UK under the Financial Services and Markets Act 2000. The FSA lays down strict requirements to protect the consumer against malpractice, and has wide investigatory and enforcement powers to ensure those requirements are observed. The FSA's regulations require all financial institutions to store all business emails sent and received for up to six years, and some emails indefinitely, so that cases can be reviewed.

Summary

Clearly, there are many reasons why an organisation should ensure that the information in its email communications is properly managed. From a practical perspective, email communications now form part of the mainstream business record of an organisation, and should be treated as such. Adequate records are essential for the efficient running of any organisation, irrespective of any legal requirement, and for those records to be of use, they must be reliably stored and capable of being retrieved swiftly and with ease.

This white paper is not intended to give legal advice, and merely seeks to give an overview of the legal issues that are relevant to the management of email records, nor does Blake Lapthorn Tarlo Lyons endorse the product of any particular vendor. Demonstrably, however, the volume of legislation that surrounds information management is growing at an ever-increasing pace as the law catches up with the march of technology. Legal and regulatory compliance issues are becoming a routine consideration for IT departments, and each organisation will need to obtain its own legal advice and assess which pieces of legislation are applicable to its operations.

Every compliance strategy will have to involve a consideration of the technical, as well as the organisational means of implementation

No compliance strategy will be effective without proper consideration of how the strategy will be implemented in practice, or of how to demonstrate that compliance. Every compliance strategy will have to involve a consideration of the technical, as well as the organisational means of implementation. Organisations need to take special care to ensure that the email archiving solution they purchase delivers the functionality needed to make the task of compliance as efficient as possible, notwithstanding major considerations like risk mitigation, best practice and corporate governance.

David Kwan, Product Manager at security specialists MessageLabs explains how the MessageLabs Archiving service can address the legal concerns of organisations in the UK:

'Our customers are relying on their email systems as the central location to exchange and store vital data. It is imperative for the productivity and security of your business that this information be securely archived and easily searchable. At MessageLabs, we provide a managed email archiving service that has the functionality necessary to help you meet all your legal and compliance needs.'

'Our email archiving solution provides a central repository that allows you to search for email across the enterprise and easily meet legal discovery requests. You can also reduce exposure to legal liabilities by implementing and enforcing an email policy with proper retention rules.'

To find out more visit www.messagelabs.co.uk/products/archiving/

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
Feringasträße 9
85774 Unterföhring
Munich
Germany

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

© MessageLabs 2005
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