E-mail and internet use at work

by Michael Hart and Ellen Temperton, Baker & McKenzie, London office

Practice notes | Law stated as at 01-May-2002 | International

This note reviews the legal risks involved in the use by employees of e-mail and the internet at work, and also considers related issues such as the implementation of a company policy for e-mail and internet use by staff, the monitoring of e-mail and internet use by staff, and requirements in relation to the disclosure and retention of e-mails.

The use of e-mail and the internet in the workplace has become widespread across virtually all industries and in businesses large and small. Employees are using these tools on a daily basis, changing the ways in which companies communicate and do business, and increasing the speed at which they can do it. However, these tools have also exposed businesses to new risks and problems.

While e-mail can enable employees to respond quickly to requests from suppliers, customers and others, businesses face difficulties in controlling the obligations which are being undertaken in such e-mail. The huge increase in the volume of e-mail correspondence flowing to and from businesses on a daily basis raises questions about the extent to which a business should keep copies of this correspondence, and how it should do so. As far as use of the internet is concerned, although it is a valuable research tool, it can also be a source of unwanted "information", whether in the form of pornography or other illegal materials imported by employees, or viruses that can cripple the computer systems on which a business depends.

Unless employees are given clear guidance relating to their e-mail and internet use in the workplace, they may waste time on non-work-related matters during the working day, and there is a risk of the employer being publicly embarrassed, having its systems and data compromised, and even being exposed to legal liability. Even if the employer is able to show that it is not vicariously or otherwise liable, the time and expense of becoming engaged in a dispute can itself be damaging to a company.

It is therefore essential to be fully aware of the risks involved in e-mail and internet use and to have appropriate legal, practical and technical safeguards in place.

The following issues are examined in this note:

- Internet use by employees.
- E-mail use by employees.
- Implementing a policy for e-mail and internet use by employees.
- Monitoring e-mail and internet use by employees.
- The circumstances in which the disclosure of e-mails may be required, and deciding which e-mails should be retained by a business.
- The risks associated with the use of intranets and extranets.

Internet use by employees

According to a paper published by International Data Corporation (IDC) in March 2000, some 122 million people worldwide have internet access at work, and it is estimated that this number will more than double by 2004.

The internet is a vast and unregulated collection of different computers, all networked to each other. The computers enable those with internet access to conference with each other, to collect files from and upload files to other computers, and to send e-mail. Internet service providers use their host computers as computers to be networked to the internet, enabling their customers to access the internet through their computers dialling in to the host. Several areas of internet use by employees can give rise to problems:

- Sending e-mail messages via the internet (the most widespread use of the internet).
- Submitting postings to internet newsgroups. Comments posted to newsgroups are more public than e-mails and, as they are accessible at the same time in many different jurisdictions, they create an even greater risk of vicarious liability for employer organisations than do e-mails.
- Surfing the world wide web. An employee who surfs the web leaves a "calling card" at each website that he visits, from which the organisation may be identified. This could cause embarrassment to the organisation if a visited site contained inappropriate material.

The main legal and practical risks arising from the use of the internet other than for the purpose of e-mail are considered below (risks associated with e-mail are discussed under *E-mail use by employees*).

Crime

There are a variety of criminal offences which employees might commit through the use of their computers, for example, criminal harassment, downloading pornography or gaining unauthorised access to a computer system (known as “hacking”). Even if an employer’s potential vicarious liability for its employees’ criminal acts is quite limited (as in the UK, for example), a company still needs to be concerned about bad press and damage to its reputation, given that an organisation may be identified from visits made by its employees to particular websites which may contain inappropriate material.

Copyright

The risk of employees infringing copyright is not new, but the risk to business has increased because of the ease with which content can be copied from the internet and then quickly and widely distributed to others. For example, employees might copy content from the internet and transfer it by e-mail without having any actual or implied licence to copy from the owner of that content. It is a simple matter for a person surfing the internet inadvertently to breach copyright by attaching a web page to an e-mail and sending it to others. In attaching such pages, or even extracts from documents, and e-mailing them to others, the sender may not include with the material any relevant copyright notices or warnings located elsewhere on the website. It is also easy for employees to ’cut’ large amounts of text and other material from the internet, and "paste" them into their own documents. These documents containing infringing material may then be circulated widely within or outside the company. It could be embarrassing for a company to be accused of breach of copyright because a large part of a company’s document is found to be an exact copy of someone else’s work.

Copyright infringement may also occur if an employee downloads music onto his workplace computer from a website which makes available infringing copies of music, and also if the employee transmits the music onwards to others. An employer should ban such uses, not least because the owner of the music may decide to sue the employer as well as the employee in order to cause embarrassment and try to promote some financial or other settlement. Napster, the US-based music sharing service, agreed in September 2001 to re-model its service as a subscription-based service and to offer only music which had been licensed for use on the service. The likelihood of copyright infringement occurring as a result of an employee's use of such a licensed subscription service is considerably reduced.

Sexual and racial harassment

In many jurisdictions there is a possibility of legal action for sexual or racial harassment through the use of e-mail. In Australia, for example, employee e-mail harassment has been held to breach anti-discrimination laws, and in the UK (where an employer has a duty to take reasonable steps to prevent an act of harassment occurring in the workplace), harassment has been held to include colleagues accessing pornography on the internet. Controls on this sort of internet use should therefore be put in place by implementing appropriate internet and e-mail usage policies which make employees aware of unauthorised uses and the disciplinary consequences which may follow (*see E-mail and internet policies*).

Cyberslacking

For many businesses, the internet is a very useful research tool. For some employees, however, the temptation to use the internet at work for non-business purposes is irresistible. Some sources claim that 30% to 40% of internet use during the ordinary working day is not business-related, and that this is when 70% of all pornographic website traffic occurs.

Companies can control non-work-related use of the internet by limiting internet access to certain controlled points within the company, such as the library, or to specific "approved" websites. However, if companies do allow internet access from staff computers, they need to decide not only whether to ban certain types of use, but also whether to regulate when or if personal use is permitted, and then make this office policy (*see E-mail and internet policies*). For example, in a UK case an employee was found to have been fairly dismissed for gross misconduct after logging on to a holiday-related internet site 150 times during working hours (*Franxhi v Focus Management Consultants Ltd(LTL 26/1/00)*).

Viruses

Material downloaded from the internet (such as screen savers) onto a company's internal network could contain computer viruses. Even if employees only have access to the internet by e-mail they can still import executable files that could contain viruses. Such viruses can be potentially catastrophic for a business' systems and data, so employees must be clearly informed of the dangers.

A frequently used technical safeguard is a "firewall". This is a set of programs located at an internet gateway server, that is not a part of the receiving party's internal network, which runs all incoming files through a virus-checker (and in some organisations subjects them to human inspection) before allowing them onto the network.

From a legal risk perspective, if crucial systems are prevented from working or vital data or documents are lost because of a virus, this could mean that a company is unable to carry out its commitments, some of which may be

contractual. In some jurisdictions, depending on the circumstances leading to the virus, the occurrence of a virus may be seen as an act of *force majeure*, and therefore as absolving the company from liability for breach of contract. However, if the virus was imported by an employee in circumstances where there was no policy in place warning that employee of the dangers of downloading material from the internet and prohibiting the employee from doing so, it would be much more difficult for the company to argue that it was an act of *force majeure*. In any event, the absence of such a policy will increase the risks of customer complaint or possible legal action against the company.

E-mail use by employees

Almost everybody with access to the internet has an e-mail account, and the number of e-mail users, which is already vast, is continuing to grow. In the early 1990s, there were 15 million e-mail accounts in the world. Messaging Online reported 569 million e-mail accounts globally at the end of 1999, up by 83% on the previous year.

A basic characteristic of communication by e-mail is the speed and ease of communication and the sense of apparent intimacy and informality which exists between sender and recipient. This sense of apparent intimacy, and the speed at which an e-mail message can be produced, often means that people will say things without thinking them through as carefully as they would if they were to write or dictate an ordinary letter. As the sender is generally alone with his computer when typing an e-mail (particularly so as more company workers “telework” from home using computers), this can lead to an even greater sense of comfort than with a telephone conversation, as the sender is not constrained by the “presence” of the other party. This can lead to a series of issues, ranging from the making of defamatory remarks to bullying or harassment by e-mail. However, unlike the average telephone conversation, e-mail messages leave a record, which can be produced in hard copy form. Many of the comments below also apply to voicemail messages left by telephone, which are also recorded, though people often tend to be more careful in what they say in a voicemail message.

The main legal and practical risks arising from e-mail use by employees are considered below.

Contracts

Employees can inadvertently form contracts through e-mail correspondence. Because of the intimacy of the process of sending messages by e-mail, there can be a danger that it lulls the communicating parties into a false sense of security which might lead to the formation of contractual obligations without the usual care and detail, or level of internal sign-off, that is required. Some of the potential pitfalls include:

Pre-contractual misrepresentation

Sales staff often make statements in order to secure a contract, which can give rise to problems if such statements are later held to have legal force. Although a seller or supplier may be able to avoid legal liability for such statements if the customer fails to have them included in writing in the contract (particularly if the seller's or supplier’s standard terms contain an "entire agreement" provision which expressly limits the enforceable terms or representations to those contained in the written document), the potential exposure of companies is greatly increased by pre-contractual representations made by e-mail, where the customer will have a written record of the statement to rely on. Even where a customer is unable to establish legal liability on the part of the seller or supplier, a copy of an e-mail containing a representation made by sales staff can at the very least be used as commercial leverage by the customer.

Employers therefore need expressly to limit their employees' authority to make representations or enter into contracts. Where pre-contractual negotiations may be conducted by sales staff using e-mail, companies should specify in their e-mail policies what sales staff can and cannot say.

Breach of contractual obligations

While formal written correspondence and faxes are often carefully filed in hard copy form, e-mails may not be filed so methodically. If a contract has been formed or a representation has been made by e-mail, and such undertakings have not been duly filed or recorded, it is easy for the company inadvertently to breach such undertakings. This is a particular issue where a company has high staff turnover or regularly moves staff to different operating units. If an employee who has given an undertaking by e-mail has moved on, without leaving a hard copy on file, the company may not be aware of its obligation until such time as a customer complains. A practical solution to this problem may be to implement a policy requiring all employees to print and file hard copies of e-mails sent and received in the course of contractual negotiations, or to incorporate software which at least prompts the sender to print an e-mail at the same time as it is sent.

Proof of contract

There may be occasions where a company wishes to prove that a contract has been formed. In the case of an ordinary letter, proof of sending is easily demonstrated by producing a file copy of a dated and signed letter and establishing that the company procedure is to send letters on the day they are dated. In the case of faxes, a print-out of the transmissions report will show whether the fax has been successfully transmitted. However, most e-mail systems have no similar print-out mechanism, and so it is important to:

- Use the facility available on e-mail programs to show that receipt has been confirmed where the company needs to know that a message has been received. Various e-mail applications have different options regarding receipt facilities, but may include a delivery receipt or a read receipt. Where available the read receipt should be used. However, it should be noted that the reliability of such facilities has not yet been clearly established.
- Make a note to check that the receipt message has been received.
- Keep a hard copy of the receipt notice.

For companies who do wish to enter into binding contracts by e-mail (notwithstanding that contracting by e-mail is not yet a widespread practice) this procedure is even more critical. There is no point in accepting an offer by e-mail, only for the other party to deny that it ever received that acceptance.

It should be noted that, in a number of jurisdictions, digital signatures have the same legal standing as written signatures (*see Practice note, Security and digital signatures: Law relating to digital signatures*). In these jurisdictions, employees using digital signatures on company e-mails will therefore have greater perceived authority to enter into contracts on the company's behalf.

Copyright

As has been mentioned above, sending copyright works by e-mail which have been copied without the consent of the rights-owner is likely in many circumstances to constitute copyright infringement. It is easy to attach copyright material to e-mails and to cut and paste attachments from other e-mails. There is an additional risk that any warnings

in the text of the original e-mail on the use of the copyright material, or restrictions on the circumstances in which it may be used or copied, may be lost when only the attachment to the e-mail is copied.

Defamation

There is a risk in many jurisdictions of liability for defamation by use of e-mail messages. Companies may be liable for defamatory comments made by employees on the basis of vicarious liability for the acts of their employees, or as publishers of the defamatory statements (by providing the medium for publication, that is, a computer with the necessary e-mail software and internet link). The fact that a statement was only communicated to another employee within the same organisation may well be no defence to an action for defamation; indeed many of the recent defamation cases in the UK, for example, relate to comments made by one employee to another via internal e-mail. It is therefore vital to have an effective policy which reduces the chances of defamatory statements being made (*see E-mail and internet policies*).

Confidentiality

Many internet users are concerned about the security of the internet. To overcome these perceived problems, many e-mail providers have established more secure means of e-mail transmission. AT&T, for example, use a mail system called X400 which is more secure and can transmit binary file attachments. In reality, the chances of messages being intercepted over the internet are very small, let alone interception by a party with the interest and wherewithal to cause damage to the sender. However, as there is technically a risk, there is no point in taking chances when dealing with highly confidential information.

Confidentiality notices should therefore be used on confidential e-mail messages (similar to those commonly used for faxes), such as:

“This document is strictly confidential and intended only for use by the addressee unless otherwise indicated.”

The purpose of such a message is to give notice of the confidential nature of the document to any unintended recipient so that, in the event of misuse of the document, there would be grounds for bringing an action for breach of confidence.

Lawyers need to be especially careful about communicating through unsecured online e-mail systems in order to ensure they do not breach their rules of professional conduct. Even if the rules of professional conduct in the relevant country permit clients to agree to this type of information delivery service, it is still advisable to send appropriate warnings on the use of e-mail transmitted via the internet, particularly where the client is not likely to be aware of the dangers.

In the EU and other countries which have similar data protection regimes, businesses must be particularly sure that their e-mail systems adequately protect personal data in compliance with their applicable national data protection legislation (*see Practice note, Data protection and privacy*).

Disclosure

In jurisdictions where disclosure of documents is required as part of the litigation process, an e-mail may be a document that is required to be produced in litigation. Regularly deleting e-mails before an obligation to disclose

arises will not necessarily be a solution: it is very difficult to delete e-mails completely, as back-up copies are automatically made and retained. The issue of disclosure and retention of e-mails is discussed under *Disclosure and document retention*.

Sexual and racial discrimination or harassment

There is often a risk of legal action for sexual or racial harassment through the use of e-mail. There is a particular risk that e-mail may be used for sending inappropriate messages, or recording statements which provide evidence of inappropriate conduct. The particular risks of harassment in the context of e-mail use must therefore be explained to employees, and there should be a specific policy prohibiting inappropriate use. In some countries (such as the UK), failure to do this could mean that an employer will be held liable for acts of harassment occurring at work.

Security

Although the chances of external breaches of system security or interception of e-mails by a third party are quite small, the possibility does exist. However, there is a greater danger that a disgruntled employee may deliberately forward sensitive information, for example, to a competitor, or to his home or private e-mail account if he is intending to become a competitor. Dangers may also come from employees "hacking" into private areas of the company network, and from software (which can be downloaded from the internet) that allows the hacking of third party e-mail.

Measures that may be taken in order to manage these security risks include conducting regular inspections of employee e-mail logs (subject to rules on monitoring) for breaches of security, the logging of access to private areas of the company network and communicating the company's policies to employees by way of an IT usage policy.

Viruses

As was demonstrated by the "Love Bug" virus (an e-mail virus that spread as an attachment to an e-mail which, when opened, automatically mailed itself to every address in the user's address book) and the rash of e-mail imported viruses which have followed, an employer's systems and information can be compromised by the importation of viruses through e-mail. There needs to be a policy warning employees of the dangers of opening unusual e-mails (for example, e-mails from any sender whose name they do not recognise). Technical measures such as firewalls may also be employed, as explained above (*see Internet use by employees*).

Congestion

The ease with which e-mails can be created means that people send e-mails for all sorts of trivial matters unless encouraged not to do so. Further, there can be a tendency to send copies to all and sundry, especially where the e-mail system has a blind copy facility. This can lead to staff accumulating large numbers of e-mails which not only wastes their time but can also eventually clog up and slow down the system. Staff should be encouraged to use internal bulletin boards when, for example, advertising the sale of a flat or sending out a request for a missing pen. Congestion can also be caused by employees e-mailing each other with pictures, video or other executable files, where the size of the attachments is very large. This is compounded if the sender copies the e-mail to a number of fellow employees.

Some employers forbid the use of the employer's computer systems for any personal purposes at all, though moderate use (the best analogy being private telephone calls) should in most cases be acceptable.

E-mail and internet policies

Having identified some of the legal and practical risks associated with e-mail and internet use by employees, the next step is clearly to minimise these risks. An essential first step is to formulate and then propagate a clear company policy on the use of e-mail and the internet. A company policy is important because, provided that the disciplinary consequences of a breach are made clear, it ensures that employees have clear guidelines as to what is and is not acceptable use, reduces the risk of the company becoming vicariously liable for the acts of its employees and ensures that the company can lawfully discipline or dismiss employees who use the internet or e-mail in an unacceptable manner. Unless the standards of conduct and performance expected of employees are made clear to them, their dismissal for internet-related offences could be unlawful.

Formulating a company policy

Short-form warning notice

Companies should produce and circulate a short, clearly-worded warning notice to all employees and consultants working for the company, telling them what they can and cannot do with regard to e-mail and internet use. In addition to liabilities incurred by employees, there is also a possibility of non-employees, such as contractors and consultants, incurring liabilities on behalf of the company. Although consultancy agreements will usually provide for the company to be indemnified in such situations, bad publicity may result and it is therefore advisable to send the warning notice to consultants and contractors as well as employees. The notice should be kept simple and, if the employer is an international organisation, foreign-language translations should be available. The message should explain that the guidelines and warnings are of critical importance and that non-compliance constitutes a very serious disciplinary matter. An example of such a notice is set out in the box: *Short-form warning regarding internet, e-mail and voicemail use*.

Short-form warning regarding internet, e-mail and voicemail use
NON-COMPLIANCE WITH THESE IMPORTANT REQUIREMENTS COULD RESULT IN SERIOUS DISCIPLINARY ACTION.

- Always exercise caution in what is said in e-mails or voicemails, as improper statements can give rise to personal or company liability.
- Never send or receive private e-mails at work which you would not want a third party to read.
- Never send abusive, obscene, sexist, racist, harassing or defamatory messages. If a recipient asks you to stop sending them personal messages then always immediately stop.
- Never send messages from another employee's computer or under a name other than your own name.

- Never send strictly confidential messages by e-mail or the internet without getting the recipient's agreement, and always add appropriate confidentiality notices to the message to give any third party notice of its confidential nature.
- Never give passwords to access office systems to any third party without permission from the person to whom you report.
- Never use the internet for non-work purposes [other than out of office working hours].
- Never download software, programs, music or other content from the internet other than for work-related purposes, and always check this first with your IT department to avoid downloading viruses.
- Always remember that music, text and other content on the internet are copyright works. Never download or e-mail such content to others unless you are certain that the owner of such works allows this.
- Never download files from the internet, or open unknown or unusual-looking e-mail messages, or attachments to unknown e-mails, without first having them properly scanned for viruses by your IT department.
- Always remember that e-mail messages are disclosable documents, which may be required to be produced in legal proceedings.
- Never agree to terms or enter into contractual commitments or make representations by e-mail without having obtained proper authority.
- Always make hard copies of e-mails, as these are necessary for record keeping purposes.
- Always avoid creating e-mail congestion by sending trivial messages or unnecessary copies of e-mails.
- Always obtain confirmation of receipt of important messages.

Full-length company policy

In addition to the short-form notice, a more comprehensive and detailed policy should be developed and, in jurisdictions where it is legally possible to do so, incorporated by reference into employees' employment contracts. A typical policy in the UK should address the following points (in some jurisdictions the approach to these issues will differ, particularly where collective consultation with works councils or unions is required):

- Explain what constitutes proper e-mail, internet and IT usage, indicate levels of acceptable use, including if and when use for personal purposes is permitted, and give examples of inappropriate use.
- Spell out the consequences of a breach of the policy, specify the likely penalties and, in particular, indicate when dismissal may follow.
- Expressly reserve the right to monitor the use at work of e-mail and the internet in the ordinary course of business, at the company's discretion. Explain the monitoring activities and how and for what purposes it is

done, the methods to be used and who to talk to about it. State whether data will be passed to third parties. Remind users that "deleted" material remains on the system and may still be monitored by the company.

- Include provision for employees to raise grievances about other employees' use of the technology.
- Check that the policy is consistent with all other company policies, such as disciplinary, anti-harassment and (where applicable) data protection policies.
- Specify that all e-mails must either be deleted, printed and deleted, and/or archived electronically as necessary when dealt with by the person receiving or sending them.
- Have appropriate warning messages to put on e-mail or internet communications. Notices at the end of e-mail messages should contain confidentiality statements indicating, for example, that the company is monitoring communications, explaining what is done with the messages and (where applicable) referring to the rights of data subjects.
- Ban the importation of home software onto the system, and explain that this is in order to reduce the risk of infecting the system with viruses.
- Address e-mail etiquette (that is, e-mails should be courteous, professional and businesslike) and provide instructions concerning corporate style.
- Provide a named contact for managing the e-mail and internet access system.
- Give instructions about passwords, encryption and permitting others to use an individual's computer.

Policies should extend not just to employees but also to "workers". Because liability could be created by individuals who are not, strictly speaking, employees, an employer will need a policy applicable to all categories of workers who have access to the employer's systems.

Companies should check their obligations towards works councils and unions. Any policy will need to be specifically adapted to the jurisdiction or jurisdictions in which the employer operates. In some jurisdictions, co-determination with works councils or unions is required before introducing such a policy (in France and the Netherlands, for example, works council approval is required for the use of a system to monitor employees). Employers should ensure that they understand what workforce demands will be before entering into the negotiation process.

Companies should ensure that their IT departments understand the employer's legal obligations. In countries with data protection laws, systems should be data protection compliant, for example, in relation to the mechanism for deleting messages on a regular basis, security, preventing unauthorised access to computer systems via the implementation of firewalls, providing private passwords for each user, and the encryption of confidential documents.

The policy should be widely publicised and should include appropriate warnings that certain breaches of the policy may be disciplinary offences and, in serious cases, could result in dismissal. This should not be limited to written warnings contained in the employee's handbook if there is a likelihood that the handbook will sit unread on a shelf. The policy could even be cross-referenced to relevant provisions in the employee's contract. The warnings should be highlighted as part of the employee's induction materials (perhaps with a signed acknowledgement), and employees should be left in no doubt that e-mails may need to be read by the employer, and monitored if abuse is suspected, or possibly monitored on a routine or random basis even if abuse is not suspected.

Insofar as the policy creates new categories of misconduct, it should be properly cross-referenced with the company's disciplinary rules. In particular, if the company's disciplinary rules contain a list of categories of acts of gross misconduct, they should be amended to include gross breaches of the e-mail and internet use policy.

When implementing your policy, consider:

- A period of consultation (which will earn goodwill with employees and perhaps flush out further or new issues).
- Training and publicity. A policy perceived to be in the interest of all, and which is proportionate to its purposes, may be supported by employees even if it permits monitoring and surveillance.
- Ensuring that all workers sign a copy of the policy so they cannot later claim they were unaware of it.
- Conducting periodic audits of usage practices. This will help to establish whether current use is in line with the stated policy and enable consistent enforcement of breaches of the policy.

Monitoring e-mail and internet use

As discussed above, inappropriate use of technology by employees can create a wide range of liabilities for an employer. Monitoring employees' use is one way of minimising those liabilities although, as has been mentioned, the risk of misuse will be reduced by establishing clear rules and expectations amongst the workforce in the first place. In many jurisdictions, employers are legally permitted (subject to appropriate conditions) to monitor their employees' use of e-mail (but not its contents) and the internet in the workplace.

While employers in many jurisdictions may monitor employee e-mails, continuous monitoring is often not permitted. In the UK, for example, continuous monitoring is likely to be seen as excessive processing of personal data under the Information Commissioner's code of practice on monitoring, and consideration should also be given to the proportionality of the monitoring in the context of the Human Rights Act 1988, which may be relevant in proceedings for unfair dismissal.

Why monitor?

There are clearly circumstances in which a company will need to look at employee e-mails. For example, the employee may be away sick, and his e-mails may be the only way of ascertaining what he has done or what needs to be done on a matter, or (in jurisdictions which have rules relating to disclosure) a disclosure request may be made for that employee's e-mails. In addition to such routine matters, a company might have reason to suspect that an employee is engaged in inappropriate e-mail or internet use, or improper behaviour, which may be evidenced in the employee's e-mails. In such circumstances, the employer may wish to monitor the employee's internet use or look at the employee's e-mails. Indeed, a company may wish to monitor internet use as a matter of course (but note the comments above regarding the dangers of continuous monitoring) to ensure that employees are not spending too much time on the internet for non-work purposes during working hours, or that pornographic or other inappropriate websites are not being accessed.

Methods of monitoring

There are various means by which employee e-mail and internet use can be monitored, and a variety of software is available to do this, for example:

- Web-filtering software, which sifts through a database of internet sites and blocks unauthorised internet addresses.
- Content-recognition software, which searches for words in context, such as "hot" and "sex", to screen out inappropriate materials.

- Keystroke loggers, which can monitor and record every keystroke and mouse-click, regardless of whether it is ever saved in a file or transmitted over a company network.

Regulation of monitoring

In many countries, for example France, the monitoring of e-mail and internet use is strictly regulated, although a some countries, such as Canada, have no specific regulation at all. Many jurisdictions permit employers to monitor e-mail communications between employees, but the position on monitoring communications between employees and external third parties is often less clear. Clearly, it is vital to ensure compliance with local legislation before any monitoring is carried out in that jurisdiction. This area is the subject of specific legislation in the EU.

Disclosure and document retention

Companies often overlook the fact that e-mail correspondence can in certain circumstances be required to be disclosed in legal actions or regulatory proceedings, irrespective of how confidential the e-mail may be. E-mails can come back to haunt you, as Bill Gates found to his cost in the Microsoft anti-trust litigation, where the following e-mail sent by him (after an earlier so-called consent decree had been agreed in the litigation) was reportedly presented in arguments: "This anti-trust thing will blow over and we haven't changed our basic business practices at all except it may change our e-mail policy." A tender or humorous e-mail sent in the height of an office romance could later become the basis of a sexual harassment claim. Companies therefore need to make their staff aware of what may have to be disclosed at a future date, and consider their document retention policies. This note deals with disclosure and document retention only in relation to e-mail, as a more general discussion of such issues is beyond the scope of this Manual.

Disclosure

Company documents, including e-mail, may have to be disclosed in three main situations:

- For the purpose of litigation (with the exception of certain privileged documents).
- In the course of an investigation by regulatory authorities (with the exception of certain privileged documents). In the EU, for example, the European Commission has powers to order disclosure of documents, including e-mail correspondence, in the context of a competition law investigation relating to possible breaches of Articles 81 and 82 of the EC Treaty.
- Following requests made by persons for access to data relating to them under EU member states' national legislation implementing the Data Protection Directive (*see Practice note, Data protection and privacy:Observance of data subject's rights*).

Deleting an e-mail is not equivalent to shredding a document. It is in fact difficult to delete an e-mail completely. Deleting it from a storage folder does not destroy the copy in the trash folder or the copy saved in a back-up file on the company's network. An infamous example of the persistence of deleted e-mail messages occurred as long ago as the late 1980s, during the US Congress's Iran-Contra investigations, when deleted e-mail correspondence between Colonel Oliver North and General John Poindexter was retrieved from White House back-up tapes. In his testimony before the Senate, Oliver North said, "We all sincerely believed that when we sent a PROFS message to another party and punched the button 'delete' that it was gone forever. Wow, were we wrong."

Even if extensive steps have been taken to delete e-mails, there are high-tech forensic specialists who are expert in recovering wiped computer records. Further, even if all copies of e-mails have been successfully deleted within the company, e-mails can, unlike paper documents, very quickly circulate outside the company by being copied to other people.

The persistence and easy onward transmission of e-mails is compounded by the fact that e-mails are often written and sent off at some speed without the sort of reflection that is given to an ordinary letter. E-mails may be written at home or late at night, when the author may feel more relaxed and off guard than when at the office. These factors all increase the risk of writing and sending inappropriate e-mails which could be damaging to the company if required to be disclosed at a later date.

Company policy on disclosure

There is no short cut for a company on how to educate its employees on what documents are disclosable and what documents are protected by privilege, as these are often complex questions. Nor is it practicable to establish a comprehensive vetting process.

What can be done, however, is to try to make both management and staff aware of a number of warning signals. All staff must be trained to exercise caution in what is said in e-mails and never to send private e-mails at work which they would not want a third party to read. They must also be made aware that all e-mail messages may potentially be disclosable in legal proceedings or in the course of a regulatory investigation, with the exception of certain categories of documents that may be privileged. Caution should therefore always be exercised, and legal advice should be sought in relation to matters which may be subject to possible legal proceedings or a regulatory investigation. This message should be communicated before any legal action is on the horizon or any investigation commences, as by then the damage may already be done.

Staff can also be encouraged to deal with matters orally where appropriate, without creating an e-mail at all, or to consider whether the list of those to whom an e-mail is copied need be as extensive as it is.

Document retention

Just as there may be cases in which the presence of unexpected e-mails causes embarrassment, there are other instances in which a company will want or may be legally obliged to retain certain records (for example, accounting or sales tax records). Although, as mentioned above, e-mails and electronic records can be difficult to delete, that does not mean that they cannot be deleted. When companies change their e-mail software, there is always a danger that important records, which would tend to be retained if stored in hard copy, will be destroyed. Companies therefore need to consider their policies for the back-up of e-mail correspondence and retention in hard copy form of important documents. This should be done in the context of the company's overall document retention policy.

Any document which comprises some form of contractual agreement or representation should be retained and be made known to the managers responsible for the matter. Companies do not want to find themselves in a position in which salesmen, anxious to secure their commission for a transaction, make e-mail representations without the knowledge of their supervising managers which only come to light at a later time. Companies should make it clear that e-mails containing or recording contractual agreements or representations need to be filed with the other formal correspondence on the transaction. Other types of communications which should also be retained are operational communications to which it may be necessary to refer in order to prove certain events or circumstances

at a later time, such as minutes of board meetings circulated by e-mail, instructions to senior management or staff and communications notifying company policy to employees.

In an age when e-mail use is increasing all the time, it is important to ensure that (in countries where it is common practice and legally permitted) there is an entire agreement clause which makes it clear that the only representations, conditions and warranties which apply are those set out in writing in the final signed agreement.

As a general rule in most jurisdictions, computer-generated records and copies of paper records generated by a computer process will be admissible as evidence, although stringent conditions usually have to be followed to make them admissible.

In jurisdictions where a disclosure obligation arises, care needs to be taken where it is standard IT practice for e-mails to be automatically destroyed on a periodical basis. This practice could result in a business being in breach of its obligation to the court without even knowing it. Indeed, the failure of a lawyer to advise his client of this obligation from the outset could become a source of embarrassment. If one party requests the other to provide details of what has happened to e-mail messages between particular individuals who are intimately involved in the case, the realisation that such documents have been destroyed could prejudice the case of the party responsible for such destruction, as this will have to be explained to the court. Further, the ultimate sanction for failure to make proper disclosure is that the party in default may be ordered to take no further part in the litigation.

Intranets and extranets

In addition to the internet, businesses are increasingly making use of "intranets" and "extranets".

Intranets are private electronic networks owned and controlled by a business, containing information relevant to the business. They are accessible only to designated members of staff and not to the general public. Intranets often have the same "look and feel" as a standard website on the internet. They are built using the same “html” programming code as internet websites, and users navigate intranets in the same way as the internet (by means of hypertext links).

Extranets are similar to intranets, except that access is made available to a pre-defined set of people external to the company, such as specific customers or suppliers.

Security and confidentiality

It is clearly essential that intranets and extranets are kept secure. Companies will need to consider both practical measures, such as firewalls and technical access controls, and legal steps necessary for achieving such security. Although not yet a widespread practice, the possibility of taking out insurance against system breaches should also be considered.

Access to the sites will be limited to specifically authorised persons who will be given special passwords. It is prudent to make it clear to persons who receive such passwords that they should be kept strictly confidential and never disclosed to third parties. A password should be invalidated when an employee leaves the company, and this should be done immediately if there is any risk that the employee may not act in the best interests of the employer before leaving.

In the case of customers or other third parties who are given access to an extranet, there should be contractual terms under which both the company and the customer agree to use all appropriate efforts (whether “reasonable” or “best”, depending upon the level of assurance which is required in the circumstances) to ensure that passwords

are restricted to the authorised persons. The customer should also agree to take full responsibility for any system breach caused by its fault or the actions of any of its employees.

An increasing number of countries have legislation prohibiting the gaining of unauthorised access to a company's computer system (commonly called "hacking").

Data protection

In the EU and other countries with similar data protection regimes, where personal data is collected from individuals as part of the operation of an extranet, it is important to ensure that the data protection policy of the business (for example, detailing the purposes for which the data is being collected and to whom it will be disclosed) is accessible from the extranet site before that personal data is collected. Ideally, the data protection policy should be in a position on the extranet site where it can be seen or at least accessed immediately before the user is asked to transmit his personal data to the business' extranet. As such a policy is likely to be quite long, it may be impractical to put all the information on the same page as the form collecting the personal data, so an acceptable alternative may be to create a hyperlink to a separate page on the site where the business' data protection policy is set out. The hyperlink should, however, clearly invite users to view the business' data protection policy before agreeing to send their personal data. The requirement to inform data subjects about the collection of personal data applies equally to in-house situations, where employees need to be made aware of the collection of their personal data, so businesses should ensure that the data protection policy is readily available to all employees.

- *Michael Hart is a partner in the IP/IT group and Ellen Temperton is a partner in the Employment group in the London office of Baker & McKenzie.*

END OF DOCUMENT

