



LEGAL RISKS: EMPLOYEE USE OF THE INTERNET AND EMAIL

A paper written for Symantec Hosted Services by Jonathan Naylor, Barrister.

FEBRUARY 2010

ABOUT THE AUTHOR

Jonathan Naylor (Barrister) handles both contentious and non-contentious employment issues ranging from advising clients on actual and potential claims to representing them at Tribunal hearings. Jonathan also advises clients on all aspects of the employment relationship including contracts of employment, transfers of undertakings, equality and discrimination law and termination of employment.

Another aspect of Jonathan's role is to present training for clients, which he does on a regular basis. Recent topics for training have included disciplinary and grievance procedures, managing sickness absence, avoiding Tribunal claims and the legal issues involved in monitoring employee use of email and the Internet.

THE ISSUE

Access to email and the Internet is a business critical application for most organisations, but the attributes that make such resources so essential inevitably generate significant risks for employers. Incidents of email and Internet misuse continue unabated.

This short summary considers some of the main risks that arise from employee use of email and the Internet, but it should be noted that this is not a comprehensive study of the topic and detailed legal advice should always be sought in specific situations.

THE LEGAL CONTEXT

The principle that underpins this area is a legal concept known as “vicarious liability”. In short, this means that an employer will usually be liable for the wrongful acts committed by their employees in the course of their employment; a principle that may also cover the acts of an employee that are incidental to their employment. There are strong policy reasons why courts generally wish to find an employer liable for the acts of any employee (the most obvious being that someone who has been injured by an employee may not be able to recover adequate financial compensation if their only claim is against an individual rather than an organisation).

Case law, such as **Mattis v. Pollock (t/a Flamingos Nightclub)**, demonstrates that courts have been willing to extend the boundaries of this principle. In **Mattis**, a nightclub doorman who had been angered by an incident that occurred while at work, left the nightclub, went to his home which was nearby, took a knife and returned to the club, later stabbing an individual who had been involved in the earlier incident and causing the victim serious injuries. Dismissing the nightclub’s arguments that the doorman had acted entirely independently of his usual employed role, the Court held that the owner of the nightclub was liable for the attack. A similar outcome occurred in **Bernard –v- Attorney-General of Jamaica** where the actions of a police officer appeared excessive and yet still attracted liability to the police service.

This type of case demonstrates that, with a sufficient link to the employment (even if indirect), employers may be liable even for extreme acts committed by their employees.

KEY AREAS

All employers will be well aware that there is a risk of “cyber slacking” whenever an employee has access to email or to the Internet, but there are other risks which are perhaps less obvious. Some of these are considered below.

Blogging

In recent years many employers have developed either specific blogging policies, or alternatively dedicated sections of Acceptable Use Policies (“AUPs”) to set down guidance as to what is acceptable in this area. There are numerous examples of employees being dismissed in relation to material on their blogs which the employers viewed as bringing the companies into disrepute. The trend for a growing number of employees to produce blogs seems set to continue, meaning that similar challenges will be faced by other employers.

Social Networking Sites

Comments made by employees on social networking sites can have a significant impact on their employers, particularly as the line between work and home life becomes increasingly blurred. One example was a senior police officer who posted personal information about his gay lifestyle on a social networking website, and (crucially in this case) added photographs of him posing in his police uniform outside a London Underground station. These pictures, alongside explicit comments about his lifestyle, caused his employers to take disciplinary action against him and meant that he was denied a promotion to Chief Inspector. Further examples include a supermarket employee who lost his job after writing an obscene remark about his employer on a social networking forum, airline staff who were dismissed following negative comments about passengers which were posted on a networking site and staff at a hospital who were suspended during an investigation into photographs taken at work which were then placed online.

Harassment

Barely a month seems to go by without a further example of employees accessing inappropriate material, such as pornography, through work computers, leading to disciplinary action by the employer (possibly including dismissal).

Employers also need to be aware of the potential for claims from other employees not involved in accessing or distributing such material, but who nevertheless may take action based around the employer’s failure to provide a safe working environment or perhaps allege that the conduct of the other employees amounts to discrimination. Such behaviour may lead to claims of unfair (constructive) dismissal and/or complaints such as sex discrimination.

One example of such conduct occurred when a global the IT company, found itself on the wrong end of a claim brought by a Miss Carlucci, who received £100,000 after succeeding in her sex discrimination complaint. The Tribunal accepted that she had been subjected to sexist emails and behaviour from her male bosses and that she was demoted after she brought a formal complaint. Employers should be particularly wary of discrimination complaints as there is no limit on the possible award of compensation that may be made.

Employers should also be aware that it is no defence to suggest that the inappropriate material or behaviour is not aimed specifically at the employee who brings a complaint. In **Moonsar v.** a transport company, the fact that pornographic material was being circulated amongst a predominantly male team, and that a female member of the team was aware of this behaviour, was held by a Tribunal to have created an “atmosphere of obscenity” following which the employee was ultimately successful in her claim for sex discrimination.

Obscenity

Material that is likely to “deprave and corrupt”, if published, may constitute a criminal offence under the Obscene Publications Act. Police investigations reveal that, unbelievably, employees may choose to use work computers in order to store material that goes beyond merely inappropriate material and may involve the commission of a criminal offence. Even if the employer was not prosecuted, the resulting negative publicity in being associated with an offence committed by an employee could be substantial.

Defamation

Employers should not fall into the trap of assuming that defamation is the preserve of celebrities and national newspapers. A well known supermarket chain paid £10,000 as part of an out of court settlement to a police officer who had alleged a libel. This had arisen because the police officer had been accused by supermarket staff of being involved in a “scam” to defraud the supermarket. Employees of the shop then circulated a warning email to other branches. The ease and speed of distribution of email meant that the libel was more widespread in this case than it might otherwise have been and this highlights both the strength and weakness of email as a method of communication.

Formation of contracts

The law in the UK requires very little formality in order to create a binding contract and there is no reason that a relatively brief email may not have this effect. An Employment Tribunal case, **Hall v.** a software company, demonstrated that a brief email from a line manager to an employee was enough to vary the contract of employment; the email clearly identifying the parties and carrying a “signature” by way of the name of the sender and recipient being visible from the email.

Such legal liability stemming from a relatively brief and informal communication can cause difficulty for employers, particularly if involved in commercial transactions. For example, an employee without authority might commit a company to a particular payment without fully appreciating what they had done. A further problem is often the difficulty of establishing an audit trail to determine the terms of any contract if any emails that would assist an organisation in this respect have been destroyed or deleted.

Copyright infringement

The author of any particular material generally has copyright in the content. The ease with which information can be obtained from the Internet and distributed by employees increases the risk of a breach of such intellectual property rights.

Confidentiality

Confidential information can be the life blood of a business and yet it may be very easy for employees to access it. If an employee is disgruntled or intends to leave the employment in the near future, they may seek to use the email system to remove confidential information from the business to be used for their own purposes at a later date.

Remote workers

Permitting employees to work from home or at sites remote from their usual place of work can have many benefits for an employer, but an assessment of the risks involved is essential in order to ensure that any arrangement is successful. Possibly because they can feel more detached from the work environment, remote workers may spend more time than their office-based colleagues accessing inappropriate websites. Such sites can include highly offensive or even illegal content and such behaviour also leaves the employer potentially exposed to malware.

An employer should conduct a risk assessment prior to any remote worker commencing work, identifying any specific steps that might be taken to mitigate possible dangers. The employer can maintain a degree of control by retaining ownership of the equipment used by the remote worker, ensuring appropriate security is used and by conducting regular checks on the equipment.

The increasing use of mobile technology such as smart phones and laptops, combined with the growth in wireless technology, also demands a response from employers to protect the security of data. Security solutions are required but organisations should also ensure that their Acceptable Use Policies deal with remote working and provide guidance to employees as to the additional risks.

In short, remote workers can present an increased level of risk and ask somewhat different questions of an employer's Internet and email security arrangements, so it is important for employers to be aware of this and adjust accordingly. While remote workers may be out of sight for much of the time, they should not be out of mind.

The legal framework

This is an area in which the law has traditionally lagged behind developments in technology and has attempted to catch up over the last decade. As such, there is now a framework of legislation such as the Human Rights Act, the Data Protection Act, the Regulation of Investigatory Powers Act and the Lawful Business Practice Regulations which all impinge on what an employer should and should not do in terms of monitoring their employees' use of email and Internet systems. In summary, an employer needs to have "lawful authority" to undertake monitoring of employees. The Lawful Business Practice Regulations provide for such lawful authority as long as the monitoring is for one or several of a number of specific purposes and the employer has made "all reasonable efforts" to inform the employees concerned that their communications may be intercepted.

The starting point for any employer grappling with this area is therefore to ensure that their AUP is clear and covers all of the areas required by the business. As advised by the Information Commissioner in his Employment Practices Code (which is not law but which is useful guidance and will be followed by Courts and Tribunals in dealing with this area) the employer should conduct an "impact assessment" to demonstrate that the organisation has identified the goal that it is trying to achieve and that it is implementing the least intrusive method of monitoring required in order to meet that goal.

For example, if you are concerned about excessive Internet usage by a particular employee, you may be able to deal with the problem simply by monitoring the overall time that the employee spends on the Internet rather than identifying the specific websites which the employee is visiting.

The AUP must be linked to the employer's disciplinary policy in order to ensure that the employer can take adequate disciplinary action when required. The importance of communicating the AUP to employees was highlighted by the case of **Copland v. United Kingdom (2007)** when an employee successfully argued that their human rights had been infringed by their employer covertly monitoring their telephone, email and Internet usage. While the circumstances of this case predated the introduction of the Regulations of Investigatory Powers Act, the employer's lack of any relevant policy or procedure clearly undermined their defence to the claim.

Where possible, automated monitoring should be used as this is less intrusive to the employee, but all employers must remember that it is their responsibility to implement the appropriate level of monitoring and advise their employees accordingly. Third party service providers can help but, ultimately, any claim would inevitably be brought against the employer.

Employers should also be aware of the enhanced powers of the Information Commissioner regarding serious breaches of the Data Protection Act. From 6 April 2010, such infringements may trigger financial penalties of up to £500,000 under new legislation which highlights the importance of compliance with the Act.

CONCLUSION

Most employers will have implemented an AUP some time ago, but this should be regularly reviewed and updated to meet any new threats. Such reviews can ensure that the policy remains relevant to what the employer is trying to do and the specific risks that they face.

The AUP should set out why the employer is monitoring (and partially this will be to protect the employee themselves against risks that might occur in the event of any misuse) and also set out penalties for any breach of the AUP, linking this to the disciplinary policy. While employees always tend to dislike the fact that employers will monitor employee usage of the corporate email and Internet systems, the employer has given the employee a powerful tool in this respect and it cannot be used without limits being enforced. Employees may appreciate the seriousness of the issues involved if the employer explains that a claim for discrimination by a fellow employee can lead to financial consequences not only for the employer but also the employee.

Clarity of thought is absolutely essential. The employer must have identified what they are trying to do and why and then frame the AUP and the monitoring that takes place in support of that policy to meet its specific needs.

ABOUT SYMANTEC HOSTED SERVICES

MessageLabs, now Symantec Hosted Services, is a leading provider of hosted messaging and web security services, with over 29,000 clients ranging from small businesses to the Fortune 500, located in 99 countries. Symantec Hosted Services protect, control, encrypt and archive communications across email, web and instant messaging. These services are delivered by a globally distributed infrastructure and supported 24/7 by our security experts. This gives a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.

For more information or to request a free trial of MessageLabs Security Safeguard, please visit www.messagelabs.co.uk/solutions

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH

Humboldtstrasse 6
Gewerbegebiet Dornach
Munich, Aschheim 85609
Germany
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

>AMERICAS

>UNITED STATES

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

>CANADA

170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA

Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE

6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN

Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130



Confidence in a connected world.