

# The Legal Guide to Employee Monitoring

by Hammonds



*The World's #1 Web & E-mail Filtering Company*

  
SurfControl®



Written on behalf of SurfControl by **Hammonds**

**→Notice**

This document serves as a guide for general information only; it should not be considered as legal advice. We make no warranty and accept no liability as to the accuracy or suitability of the guidelines contained herein. We advise organisations to seek individual legal advice prior to any implementation.

# The Legal Guide to Employee Monitoring

by Hammonds



Sue Nickson, partner and national head of employment law at Hammonds looks at the importance of having an Internet policy.

The subject of monitoring in the workplace always catches the interest of the press. It was back in 2000 but everybody still remembers the lewd e-mail sent to a Norton Rose lawyer from his girlfriend, which was forwarded to six colleagues and ended up being circulated worldwide. At the same time the Royal and Sun Alliance was reported as having suspended numerous insurance workers over the circulation of an obscene e-mail of the cartoon character Bart Simpson. The stories keep appearing and this year Hewlett Packard is reported to have sacked two and suspended a further 150 for viewing and sharing inappropriate material. An NOP survey on behalf of SurfControl shows that even two years after the implementation of strict rules regarding the processing of e-mails 70% would open e-mail they suspect to be inappropriate and even worse that 42% would circulate the offensive material to colleagues and friends.

The Human Rights Act 1998 came into force in October 2000 and implemented in the UK the European Convention on Human Rights (the Convention). The potential consequences for employers were clear from the decision of the European Court of Human Rights in the case of *Halford v United Kingdom* 1997 IRR471. Alison Halford, a senior police officer, alleged that her employer had tapped her private work telephone. She successfully claimed that this was a breach of her right to privacy under Article 8 of the Convention. It was held that as her employer had not given her any prior warning that her telephone calls were liable to interception, she would have had a reasonable expectation of privacy for calls made on the private facility her office provided. The fact that the calls were made from the workplace did not mean that her right to privacy did not apply. It follows that the same principles will apply to e-mail communications and Internet use as to telephone calls.

At the same time that the Human Rights Act came into force the Regulation of Investigatory Powers Act 2000 ("the RIP Act") updated the legislation governing the interception and monitoring of communications. It provided for both civil and criminal liability and made it unlawful to intentionally intercept communications over a public or private telecommunications system without lawful authority. A defence would only be available if it was reasonably believed that both parties to the communication consented to the interception. Recognising that this would prevent monitoring of most workplace communications further regulations were issued authorising the monitoring of communications where reasonably required for business purposes.

# The Legal Guide to Employee Monitoring

by Hammonds

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Regulations") provided that an employer retains the right to carry out monitoring despite the fact the employee has not given their express consent, if such monitoring is required to carry out the following:

- recording evidence of business transactions
- ensuring compliance with regulatory or self-regulatory guidelines
- maintaining the effective operation of the employer's systems (e.g. preventing viruses)
- monitoring standards of training and service
- preventing or detecting criminal activity
- preventing the unauthorised use of the computer/telephone system - i.e. ensuring the employee does not breach the company's e-mail or telephone policies.

Nonetheless, the Regulations provided that it would be necessary for an employer to take reasonable steps to inform employees that their communications might be intercepted.

On 11 June 2003 the long-awaited Part 3 of the Data Protection Code on Employment Practices, entitled "Monitoring at Work" was published. This gives guidance on how employers should comply with the provisions of the Data Protection Act 1998. The interception of e-mails is a form of data processing and therefore the employer has to consider whether the monitoring intrudes unnecessarily on the employee's privacy. The Code suggests that employers should:



- actively consider whether the risk which monitoring is designed to address justifies the intrusion into individuals' privacy by monitoring
- limit monitoring to traffic data rather than the contents of communications
- undertake spot checks rather than continuous monitoring
- as far as possible, automate the monitoring so as to reduce the extent to which extraneous information is made available to any person other than the parties to a communication
- target monitoring on areas of highest risk

# The Legal Guide to Employee Monitoring

by Hammonds



The Code provides benchmarks that employers are expected to meet in order to comply with the Data Protection Act. It is clear that in any prosecution or other enforcement action account will be taken of the employer's regard for these particular benchmarks and the uncontested first benchmark for employers is to:

"Establish, document and communicate a policy on the use of electronic communications systems."

There is a clear and absolute need for employers to have an acceptable use policy in place that is made known to all their employees.

The risks that an employer will face if they do not put into place such a policy can be seen from the decision in the case of *Dunn v IBM United Kingdom Ltd* ET Case Number 2305087/97. Here the employee was summarily dismissed for accessing pornography on the Internet. The tribunal upheld the claim for unfair dismissal as it was not a case where there was a clear breach of company policy such as to automatically warrant summary dismissal. The uncertainty that an employer faces with such an unfair dismissal claim can be avoided with a policy that complies with the following minimum requirements:

- Is in writing
- Is clearly communicated to all employees
- Sets out permissible uses of both e-mail and Internet
- Specifies the prohibited/inappropriate uses
- States what monitoring, if any, will take place
- Sets out acceptable on-line behaviour
- Stipulates unauthorised access areas
- Sets out privacy rules in relation to other users
- Sets out privacy rules in relation to employer's right to monitor and the nature and extent of such monitoring
- Stipulates possible disciplinary consequences for breach of rules

# The Legal Guide to Employee Monitoring

by Hammonds



It is an area that cannot be ignored as even leading companies have found to their cost. In the majority of the cases the offensive material being viewed or passed on is pornographic. The employer who doesn't deal with this issue may be at risk of facing constructive dismissal, sex discrimination claims or even criminal prosecution. In the case of *Morse v Future Reality ET*: Case No. 54571/95 it was held that the downloading and viewing of sexually explicit images in the workplace by male workers did constitute sexual harassment if it makes the working environment uncomfortable for a female co-worker. It's worth remembering that compensation for sex discrimination is not capped.

In conclusion employers who fail to put in place a relevant policy are at risk of a myriad of different claims both civil and criminal.

All Internet content you read, send and receive carries a risk!

SurfControl Web & E-mail Filter give you the tools you need to implement and enforce your own Acceptable Use Policy.

Only SurfControl gives you **THE TOTAL SOLUTION** for comprehensive protection against harmful and inappropriate Internet content risks.

**Download and install your FREE no-obligation 30 day trial of SurfControl Web & E-mail Filter now**

*Discover what your Web and E-mail system is really being used for. You'll be amazed!*



**+44 (0) 1260 296150**



**[www.surfcontrol.com/go/uklegal](http://www.surfcontrol.com/go/uklegal)**



## All Internet content we read, send & receive carries a **RISK!**

Harmful and inappropriate Internet content could jeopardise your:

• **security** • **productivity** • **bandwidth** • **legal liability**

Only SurfControl gives you **THE TOTAL SOLUTION** for comprehensive protection against Internet content risks!



**Download and install your FREE no-obligation 30 day trial of SurfControl Web & E-mail Filter now**

Discover what your Web and E-mail system is really being used for. You'll be amazed!



**+44 (0) 1260 296150**



**[www.surfcontrol.com/go/uklegal](http://www.surfcontrol.com/go/uklegal)**

The World's **#1** Web & E-mail Filtering Company

  
**SurfControl®**