



Internet Monitoring and Workplace Privacy Legislation (United Kingdom)

This document outlines legislation that regulates Internet and network monitoring in the UK. Organizations that are using or intending to implement a form of electronic monitoring can use this document as a starting point to determine their legal rights and responsibilities.

This document is intended as a guide only. It aims to introduce the reader to issues that may be relevant to their organization, and to point out sources from which more detailed information may be obtained. It is **NOT** a substitute for professional legal advice.



WebSpy and Privacy

WebSpy products are used by organizations around the world to monitor the usage of shared electronic resources by their members. This monitoring enables organizations to verify that the resources they provide are being used for the purposes for which they are intended. For any organization currently employing or intending to employ a form of electronic monitoring, it is useful to be aware of current privacy legislation and the effect that it may have upon your monitoring practices.



Current Privacy Legislation in the UK

There has been some confusion in recent years as to what is the governing legislation for Internet and network monitoring within organizations in the UK. There have been a number of regulations introduced that empower organizations to conduct extensive surveillance on their members without their consent. There has also been legislation proposed that contradicts these regulations.

The following legislation applies to the monitoring of individuals in an organization:

- Data Protection Act 1998,
- Freedom of Information Act 2000,
- Regulation of Investigatory Powers Act 2000, and
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

It has been argued that the principles within the Human Rights Act 1998 also have relevance to the issue of member monitoring. However, the Act does not directly apply to this matter.

There is also a draft Code of Practice that is under revision that may have some implications for organizations involved with Internet and network monitoring.

Data Protection Act 1998

The Data Protection Act 1998 (DPA) came into force on 1 March 2000. It sets rules for processing personal information held on computers and on some paper records.

The Act applies to 'personal data'. Personal data covers both facts and opinions about the individual, as well as information regarding the intentions of the data controller towards the individual.

The DPA essentially gives legal rights to individuals (data subjects) with respect to their personal data processed by others (data controllers). The DPA enforces the eight data protection principles that essentially state that data must be:

- 1 Fairly and lawfully processed
- 2 Processed for limited purposes
- 3 Adequate, relevant and not excessive

- 4 Accurate
- 5 Not kept longer than necessary
- 6 Processed in accordance with the data subject's rights (as outlined in the DPA)
- 7 Secure
- 8 Not transferred to countries without adequate protection

Organizations should also be aware that the Freedom of Information Act 2000 ("FoIA") makes various amendments to the DPA, with respect to the disclosure of information.

The Regulation of Investigatory Powers Act 2000

Part I of the Regulation of Investigatory Powers Act 2000 (RIP Act) makes it unlawful for employers and others to intercept communications in the course of their transmission on a private telecommunications system unless:

- The parties to the call, email or other communication have both consented to the interception or,
- The interception is of communications taking place in the course of the carrying on of the employer's business and is authorized under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

The RIP Act only restricts access to the contents of a communication. It does not address the collection and use of traffic data on a private network. This is subject only to the requirements of the Data Protection Act 1998.

Employers believed this Act was not strong enough as it did not permit them to do whatever might be necessary to protect their assets. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 was introduced to address this matter.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

These regulations (often referred to as LBP) permit organizations, from 24 October 2000, to monitor and/or record many communications without consent in order to:

- Establish facts relevant to the business
- Ascertain members' compliance with the law and/or self-regulatory policies and procedures
- Ascertain whether member attained the organization's standards
- Prevent or detect crime
- Investigate or detect unauthorised use of the telecommunications system
- Ensure the system's effective operation

The LBP permitted organizations to monitor but not record communications without consent in order to:

- Determine whether or not communications are business-related
- Monitor communications to a confidential support help line

Employee rights groups were opposed to these regulations, as they believed the regulations gave organizations the right to do virtually anything they wished. The groups argued that it was drafted too broadly and breached individuals' rights under Article 8 of the Human Rights Act 1998. The Data Protection Commissioner drafted an Employer Code of Practice in October 2000 to deal with these concerns.

The Human Rights Act 1998

The Human Rights Act 1998 (HRA) came into effect in 2000 to incorporate the principles of the European Convention for the Protection of Human Rights into UK law.

Under this act, Individuals have the right to:

- Not be discriminated against on grounds of sex, race, religion and political opinion
- A fair trial
- Respect for privacy and family life
- Freedom of thought, conscience and religion
- Not be tortured or subject to inhuman or degrading treatment

Draft Code of Practice

The Draft Code of Practice (the use of personal data in employer/employee relationships) is aimed at employers and is intended to be of general application. It addresses the use of personal information that is likely to arise in any employer/employee relationship from recruitment through to termination and beyond.

The Code of Practice has been drafted in two parts. The first sets out the standards which must be met to ensure compliance with the code, and the second sets out the interpretation of the Data Protection Act 1998 on which the standards are based.

There has been wide disagreement with the contents of this code, and it is under revision in an attempt to incorporate the comments received from outside parties.



Implications for Monitoring

The presence of the LBP gives extensive monitoring powers to organizations. Monitoring products such as those offered by WebSpy can be used as long as the purpose of the monitoring falls within the scope of the regulations.

However, when the Code of Practice is finally published, it is expected that the regulations within the LBP will be restricted to ensure that any intrusion into a member's privacy or autonomy is in proportion to the benefits or potential risks to the organization.

This is a long running debate that has important implications for organizations. Members may be able to claim constructive dismissal if they can prove that they

have been monitored inappropriately or incorrectly. Tribunals may also be able to refuse the admission of such evidence.

Responsibilities of Organizations

In addition to the LBP, those who decide how and why personal data are processed (data controllers) must comply with the data protection principles and the other requirements of the Data Protection Act.

The public should be able to find out who is processing personal data and other information about the processing, such as the purposes of the processing. Most data controllers therefore need to notify the Data Protection Commissioner, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data is transferred.

This information is made publicly available in a register. Data Controllers must comply with the data protection principles even if they are exempt from the requirement to notify. Exemptions are listed in part IV of the Act. Failure to notify is a strict liability offence.

Protection for Members

Due to the introduction of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 empowering the monitoring rights of organizations, the main source of protection for members in relation to Internet and network monitoring comes from the Data Protection Act.

Organizations therefore need to be aware of their members' rights under the Data Protection Act. These rights include:

- **The right of subject access**
Individuals have the right to find out what information is held about themselves on computer and paper records.
- **The right of rectification, blocking, erasure and destruction**
Individuals have the right to apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.
- **The right to prevent processing**
Individuals have the right to ask a data controller to stop, or to not begin, processing personal data where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.
- **The right to prevent processing for direct marketing**
Individuals have the right to ask a data controller to stop or not to begin processing personal data for direct marketing purposes. This is an absolute right.
- **The right to compensation**
Individuals have the right to claim compensation from a data controller for damage or damage and distress caused by any breach of the Data Protection Act. Compensation for distress alone can only be claimed in limited circumstances.

- **Rights in relation to automated decision-taking**

Individuals have the right to ask a data controller to ensure that no decision that significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

WebSpy Ltd. recommends that organizations develop comprehensive privacy and Acceptable Internet and Email Usage policies, and communicate these policies to their members. This privacy policy should at least state the methods and purpose of any monitoring taking place.



Criminal Offences

The following offences are enforceable under the Data Protection Act 1998:

- **Notification offences**

It is an offence for a data controller not to notify the Data Protection Commissioner either of the processing being undertaken or of any changes that has been made to that processing.

- **Procuring and selling offences**

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorization. This covers unauthorized access to and disclosure of personal data. There are some exceptions to this.

- **Enforced subject access offence**

It is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person for specified purposes, such as a precondition to employment, unless one of the limited statutory exceptions apply.

- **Other offences**

It is an offence to fail to respond to an information notice or to breach an enforcement notice. Unauthorised disclosures by the Commissioner or the Commissioner's staff are forbidden.



Developments

A recent proposal from the Data Protection Commissioner is currently under consideration whereby Internet Service Providers (ISPs) should preserve email communication and traffic data for law enforcement purposes. This proposal has come about because email data is easily deleted and subject to short retention periods. This can hinder police investigations when suspects become aware they are under investigation. The Commissioner warned that "this would be acceptable provided that strict conditions were laid down in national law prescribing the specific circumstances in which an order or notice could be issued on an ISP".

There is concern over the increasing usage of public registers for commercial purposes due to technological advances. Companies are accessing publicly available records, and selling them in a format that is attractive to marketers and other companies (such as CD-ROM). The Data Protection Commissioner has stated that she sees it as important that steps are taken to protect those whose details appear in public registers.



Resources

There are many useful resources on the web to help you find out about privacy legislation. However, it is always good practice to verify any information you find.

Legislation

- The Data Protection Act 1998
<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>
- The Regulation of Investigatory Powers Act 2000
<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
<http://www.hmso.gov.uk/si/si2000/20002699.htm>
- Human Rights Act 1998
<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Related Organizations and Interest Groups

- Privacy International
<http://www.privacyinternational.org>
- Privacy Organisation
<http://www.privacyexchange.org>
- Privacy Foundation
<http://www.privacyfoundation.org>
- International Labour Organization
www.ilo.org
- Labour Start
<http://www.labourstart.org>
- Electronic Privacy Information Center
<http://www.epic.org>

Other

- The homepage of the Information Commissioner
<http://www.dataprotection.gov.uk/>
- Model Acceptable Use Policy
<http://www.efa.org.au/Publish/aup.html>



All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Other product and company names herein may be the trademarks of their respective owners.