

## E-Security Overview

### Interception and Monitoring of Communications in FE and HE

Betty Willder

04 April 2006

**Please note:** this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

#### Table of Contents

1. Introduction.....	1
2. The Legislation.....	2
3. Interception.....	4
4. Lawful Authority .....	5
5. Acquisition and Disclosure of Communications Data.....	7
6. Retention of Communications Data .....	7
7. Surveillance .....	7
8. Encryption and Powers of Decryption .....	8
9. Liability and Sanctions .....	8
10. Conclusion .....	9

#### 1. Introduction

This overview paper briefly explains the current law surrounding the rights, obligations and liabilities of a college or university with regard to interception and monitoring of communications on or using its computer systems.

Interception and monitoring legislation is a potentially contentious area in FE and HE where there are prevailing traditions of privacy, independence, individualism and academic freedom.

The continuing advances in, and increase in use of, communications technology have made it easier, as well as necessary, to intercept and monitor. It is therefore important to strike a balance between this need (e.g. by the police for the prevention or detection of crime, or by the college or university itself for operational purposes) and the privacy and freedom of expression rights of the individual whose communications may be intercepted. New laws were therefore introduced to take account of these advances in technology and to attempt to address the interests of both camps. These laws supersede much of the previous law in this area. It is interesting at the outset to note that the Law Lords have stated in a recent judgement

that the RIPA is difficult legislation to interpret and consider that rather than taking too literal an approach when trying to do so, the purpose behind the Act should be considered. Attorney General's Reference No 5 of 2002 [2004] UKHL 40 available from <http://www.publications.parliament.uk/pa/ld/ldjudgmt.htm>.

## **2. The Legislation**

### **2.1 Primary Legislation**

The two main pieces of legislation in the UK with regard to interception of communications are:

The Regulation of Investigatory Powers Act 2000 ('the RIPA')

<http://www.opsi.gov.uk/acts/acts2000/20000023.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

<http://www.opsi.gov.uk/si/si2000/20002699.htm>

In addition readers operating under the jurisdiction of the laws of Scotland should note that the Regulation of Investigatory Powers (Scotland) Act 2000 works in conjunction with the RIPA and deals primarily with the authorisation system for covert surveillance in Scotland.

<http://www.opsi.gov.uk/legislation/scotland/acts2000/20000011.htm>

The explanatory notes to the RIPA state that the main purpose of the legislation is to ensure that the relevant permitted investigatory powers are used in accordance with human rights.

These investigatory powers covered by the RIPA are:

- the interception of communications
- the acquisition of communications data (e.g. billing data)
- intrusive surveillance (on residential premises/in private vehicles)
- covert surveillance in the course of specific operations
- the use of covert human intelligence sources (agents, informants, undercover officers)
- access to encrypted data

The area of the law currently of most concern to FE and HE is contained in Part I of the RIPA and the main focus in this paper is (i) unlawful and authorised interception of a communication, and (ii) acquisition and disclosure of communications data.

### **2.2 Public and Private Communication Systems**

Part I of the RIPA covers both private and public communications systems. Again it should be noted that there is still a major interpretative issue regarding what is a public and what is a private system and activity on one may closely relate to the other, rendering the differentiation difficult. The majority of FE and HE in the UK are connected to the JANET network (and accordingly have a '.ac.uk' address). For the purposes of the RIPA, it has been assumed so far that the JANET network falls

within the definition of a **private** communications network (the law regarding interception on a **public** communications network is more onerous). However as technologies converge and interoperate, the distinction may become increasingly blurred. It is by no means a cast iron guarantee that all activity on JANET would be interpreted as being on a private network, for example where interaction with a public network arises it may be a matter of interpretation in the particular circumstances. The information given here will focus on the law as it affects a private network.

## 2.3 Other Related Legislation

The following are also of relevance:

- **The Data Protection Act 1998** This legislation places obligations on how a college or university handles personal data and gives an individual some rights over how his personal data is handled. This is the law which is relevant when handling any personal data once it has been intercepted, i.e. delivered to the recipient or stored. <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>
- **The Privacy and Electronic Communications (EC Directive) Regulations 2003** These regulations make it necessary to inform web site users of how cookies and other tracking devices are used on websites. They also extend controls on unsolicited direct marketing to all forms of electronic communications. They are of most relevance from a data protection stance. <http://www.opsi.gov.uk/si/si2003/20032426.htm>
- **The Human Rights Act 1998** includes the right of an individual to privacy of communications. The provisions of every subsequent UK law should be compatible with this Act. <http://www.opsi.gov.uk/acts/acts1998/19980042.htm>
- **The Anti-Terrorism Crime and Security Act 2001** For the purposes of the information covered in this paper, this act introduces legislation purporting to enforce retention of communications data. It was brought in after the 9/11 terrorist attack in the US and already part of the Act has been repealed as it was incompatible with the Human Rights Act 1998 (and has been replaced with the Prevention of Terrorism Act 2005.) <http://www.opsi.gov.uk/acts/acts2001/20010024.htm>
- **The Computer Misuse Act 1990** This Act prohibits unauthorised access by both internal and external people to the organisation and as interception might involve unauthorised access, an offence could be committed under this Act. [http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm)
- **The Terrorism Act 2006** came into force on 30 March 2006 and has attracted much criticism. It aims to outlaw incitement to terrorist activities and will include incitement through websites and email communications and is of relevance to the educational sector. <http://www.opsi.gov.uk/acts/acts2006/20060011.htm>

## 2.4 Codes of Practice

There are also codes of practice relevant to this area of law:

- **Interception of Communications Code of Practice.** This is the code which those public authorities entitled to obtain a warrant to intercept under the RIPA (e.g. police) should follow when intercepting communications under the RIPA.

<http://www.homeoffice.gov.uk/docs/ioccp.html> The Home office has also published (10 March 2006) a revised 'Acquisition and Disclosure of Communications Data Revised Draft Code of Practice' ahead of a public consultation <http://security.homeoffice.gov.uk/news-and-publications1/publication-search/ripa-cop/acquisition-disclosure-cop.pdf>

- **The Employment Practices Code** and supplementary guidance. The code produced by the UK Information Commissioner which contains a section (Part 3) on monitoring at work <http://www.informationcommissioner.gov.uk/eventual.aspx?id=437>
- **Retention of Communications Data Voluntary Code of Practice** This code of practice again is currently assumed not to apply to UKERNA who provide the JANET network but may be of relevance to those who have other service providers. <http://security.homeoffice.gov.uk/surveillance/>  
<http://www.opsi.gov.uk/si/si2003/draft/5b.pdf>

### 3. Interception

#### 3.1 Interception by a College or University under Part I of the RIPA on its private communications network

The RIPA at Part 1 essentially provides that

- to intentionally and without lawful authority
- intercept a communication on a **private system** in the course of its transmission
- ...**is a criminal offence**

Unless the person intercepting is

- a person with a right to control the operation or the use of the private system; (for example the college principal) or
- has the express or implied consent of such a person to make the interception (for example the IT systems manager on authority of the college principal)

In these two cases it should also be noted that, whilst it may not be a criminal offence for these persons to intercept, there may be grounds for a civil action by the sender or recipient (or intended recipient) if there is no **lawful authority** (see below) to intercept.

#### 3.2 Interception by a third party

In addition, interception with the authority of a warrant is permitted for specific purposes, for example prevention or detection of serious crime. The third party must have a valid warrant in order to intercept.

Third parties entitled to apply to the Secretary of State for such a warrant to intercept are named in the RIPA and include the police and customs and excise:

- They can obtain an interception warrant allowing them to intercept communications on the JANET network.
- The RIPA at s8 details what information the warrant should contain
- The most likely reason for the grant of the warrant is that it is in the interest of national security or that it is for the purpose of preventing or detecting serious crime
- Colleges and universities if presented with such a warrant are obliged, if requested, to provide reasonable assistance with carrying out the requirements of the warrant – non compliance is a criminal offence
- Confidentiality on the part of the college and university is also a requirement – again non compliance is a criminal offence

There is more detail on third party interception and rights and duties of colleges and universities in our publication titled 'Monitoring and Encryption - the Powers of Law Enforcement Agencies' by Gavin Sutter which you will find listed on our publications page at <http://www.jisclegal.ac.uk/publicationspage.htm>.

### **3.3 What is interception in the course of transmission?**

Interception is defined widely in the RIPA and includes making some or all of the contents of the communication available, to someone other than the sender or intended recipient. There is some legal argument as to whether emails which have been read by the intended recipient but which are still stored where they can be accessed by others, for example on a university central server, are still 'in the course of transmission'. The interaction with the Human Rights Act 1998 would suggest yes, but the Employment Practices Code of Practice at paragraph 3.2.2 suggests the opposite. Unfortunately there is no case law as yet to give us a more definitive legal answer. Perhaps colleges and universities would be wise to adopt the pragmatic approach: to consider communications as being potentially subject to interception in the course of transmission in terms of the RIPA until they are filed as a record. In either event the interception of any personal data is then required to be handled in accordance with the data protection regulations.

## **4. Lawful Authority**

### **4.1 Lawful authority to intercept**

If an interception is made by '**lawful authority**' then the likelihood of civil or criminal liability arising under RIPA is much reduced. A college or university should therefore aim to ensure it has lawful authority to intercept a communication in the course of transmission. Lawful authority is provided through legislation e.g. the RIPA and also The Lawful Business Regulations. For example a valid interception warrant obtained in accordance with the RIPA provides lawful authority.

### **4.2 Lawful authority by means of the RIPA**

The RIPA allows colleges and universities to carry out the following interceptions without the consent of the sender or the receiver of the communication:

- the interception by or on behalf of the person running a service , for the purposes connected with the provision of the service – a possible example might be readdressing wrongly addressed email, or checking subject lines in email for viruses.
- The monitoring of system traffic to ensure effective performance – a possible example might be finding out the source to cut down spam

### **4.3 Lawful authority by means of the Lawful Business Regulations**

The Lawful Business Regulations at s3 provide the main source of lawful authority for interception of communications and permit the monitoring or keeping a record of communications for certain purposes. These Regulations expand on the permitted interceptions provided for by the RIPA and were the result of a Department of Trade and Industry public consultation exercise following the concerns raised by many organisations as to the restrictive nature of the RIPA.

The purpose of the Lawful Business Regulations is to allow exceptions to the basic principle of non interception as stated in the RIPA, and to allow interception without consent in certain instances.

Interception is permitted to:

- Establish the existence of facts. This is thought to mean to establish the existence of facts relating to ascertaining compliance with regulatory or self regulatory practices or procedures. Given the proportionate and purposive approach suggested by the Law Lords to the RIPA, it is unlikely to mean to establish any fact whatsoever!
- Ascertain compliance with regulatory or self regulatory practices or procedures. A possible example might be HESA reporting
- Ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system
- Investigate or detecting unauthorised use of the communications system
- Prevent or detect crime, or in the interests of national security
- Ensure the effective operation of the system

Monitoring but not recording is also permissible in the following cases:

- To ascertain whether the communication is business or personal
- To protect or support helpline staff

There are also additional conditions:

- the interception must be made solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business i.e. relevant to the business of an FE or HE establishment
- every effort must have been made to inform users that this monitoring and recording may take place

If the proposed interception by your educational establishment does not fall within one of these excepted categories, then consent of all parties must be obtained prior to any interception taking place.

As a final thought, it must not be forgotten that the Human Rights Act should lead to a narrow interpretation of both the exceptions under RIPA and the permitted acts under the Lawful Business Regulations. Therefore colleges and universities should always take care not to take disproportionate action. Some communications may also involve confidential relationships and the exceptions and permitted acts are unlikely to justify excessive or unlimited interference.

## **5. Acquisition and Disclosure of Communications Data**

The RIPA in Part 1 chapter II also sets out rules regarding acquisition and disclosure of communications data. Communications data refers mainly to traffic data and not to the content of messages. This includes numbers dialled, email addresses, and time of communications, but not the content of messages.

Certain public authorities (for example the police, the Inland Revenue, Customs and Excise authorities) may request that communications data is obtained by a service provider and disclosed to them for specified purposes e.g. prevention of crime. An education establishment required to obtain and disclose this data should only do so on receipt of a formal notice from the requesting authority. Details of the content requirements of such a formal notice are set out in the RIPA at s23.

## **6. Retention of Communications Data**

At the time of writing (April 2006) there is no compulsory retention requirement in UK law. However, there is ongoing discussion with regard to compulsory retention by service providers of communications data for a prescribed period of time. The Anti-Terrorism Crime and Security Act 2001 s104 gives the government power to invoke a compulsory retention period, but to date no legislation has been passed. Following the London bombings in July 2005 the issue has once again been raised both in the EU forum and UK, and it is becoming more likely that some measure of compulsory data retention might find its way onto the statute book. At present there is a voluntary code of practice which public service providers are requested to follow. This is on the Office of Public Sector Information web site at <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> where annex A details varying retention periods depending on the type of data. The maximum period is twelve months. To date it has been asserted that this code does not apply to the JANET network, on the assumption that it is a private network, and we will maintain a watching brief on this for any change.

## **7. Surveillance**

Surveillance is covered by Part II of RIPA and for those working under the Scottish jurisdiction, should be read alongside the Regulation of Investigatory Powers (Scotland) Act 2000. This section of the RIPA provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities of covert surveillance, agents, informants and

undercover officers. If aware of the surveillance, colleges and universities should ensure that valid authorisation is in place.

Authorisation should only have been granted in certain circumstances such as in the interests of national security or for the purpose of preventing or detecting crime or of preventing disorder. The authorisation must be necessary and proportionate to what is to be achieved by it. It also must specify a description of the direct surveillance and it has to be carried out in the circumstances described in the authorisation and for the purposes described in the authorisation.

It is to be hoped that requests for such surveillance will be limited in the further and higher education sectors, but it may be wise for an institution to have a verification procedure and allocated senior personnel to deal with any such requests.

## **8. Encryption and Powers of Decryption**

Encryption is covered by Part III of the RIPA and the powers under this section of the Act are not yet in force. At the time of writing there is no indication of a commencement date.

Colleges and universities may at present use protection techniques to send sensitive material e.g. to other researchers or sponsors, and it is important that they are aware of the powers under the RIPA for government and other agencies to request decryption thus raising issues of security and confidentiality of valuable information.

In general terms, s49 of the RIPA allows an authorised person (e.g. police, security and intelligence agencies) to serve notices (a s49 notice) on individuals or bodies (e.g. colleges and universities). These notices require disclosures, in an intelligible form, to be made of protected information which they lawfully hold or are likely to hold

There is more detailed information on this area of the law in the paper titled 'Monitoring and Encryption - the Powers of Law Enforcement Agencies' by Gavin Sutter which you will find listed on our publications page at <http://www.jisclegal.ac.uk/publicationspage.htm>.

## **9. Liability and Sanctions**

If a college or university intercepts communications on its own private telecommunications system, outwith the parameters of the RIPA, it risks incurring civil liability for unlawful interception. The result of this is that the sender, recipient, or intended recipient, may sue the college for damages. For example, where an employee believes that their employer has unlawfully intercepted an e-mail to a third party, either the employee or the third party may sue the employer.

Furthermore a staff member of the college may be guilty of a criminal offence if he deliberately and without the consent of the person with the right to control the network, intercepts a communication. A person who is found guilty of this offence is liable to a maximum of two years imprisonment or a fine or both.

Breach of the RIPA could prove costly for a college or university in terms of loss of reputation as well as financial loss.

## 10. Conclusion

The Regulation of Investigatory Powers Act 2000 was brought into force to update the previous legislation in this area and to offer the individual some protection against unlawful interception of his communications. It also regulates the extent to which government and other official agencies may intercept communications on public and private networks.

The RIPA and the corresponding statutory instruments do not give carte blanche to educational establishments themselves to intercept communications on their private systems. Any interception must be carried out within the limits set out by the legislation and those likely to be subjected to interception should, as far as is reasonably possible, be made aware that it may take place.

Modern technology has provided the means to distribute information more easily and widely than perhaps intended and this may result in offensive, or more seriously illegal, acts being committed. As well as compliance with the RIPA, colleges and universities also need to be proactive in promoting acceptable use of their communications facilities by their users.

### Further Useful Reading

Rosemary Jay and Angus Hamilton: Data Protection Law and Practice (second edition) ISBN 0-421-79480-1 for the relationship between the RIPA and Data Protection

The APiG Data Retention Enquiry <http://www.apig.org.uk/archive.html> in the 2003 Archive

The Home Office website – security section at <http://www.homeoffice.gov.uk/security/> for information on terrorism legislation

**Betty Willder**

04 April 2006

© JISC Legal - [www.jisclegal.ac.uk](http://www.jisclegal.ac.uk)