London Business School

September 2021

LBS Information Security Policy

Supporting Policy 5: Monitoring computer and Network Use

Approved by Management Board

1 Introduction

There are circumstances where LBS may monitor or record communications made using its computer and telecommunication systems, or examine material stored on those systems. This document sets out LBS's policy in respect of such activity.

It is important to be aware of the distinction made between:

- intercepting information in transit - email messages being sent, for example, or watching the web pages visited - here the relevant law is found in the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR); and
- examination of material stored on a computer - the law applicable here may vary according to variables such as who owns the computer, what material is being examined, and how the material is examined. However, the Human Rights Act 1998, and the Data Protection Act 2018 provide an overarching framework to protect the individual's right to privacy.

Under the Regulation of Investigatory Powers Act 2000, unlawful interception of communications on the LBS computer network may lead to criminal proceedings against an individual operating without the institution's authority; unlawful interception may also lead to civil action against the institution where the institution authorized the interception. The RIPA and LBPR do, however, allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks - in other words, they provide 'lawful authority'.

2 Scope

The part of this policy covering the interception of information applies to any communication on or through LBS's computer systems - the latter term being taken to include all components of the network as well as the devices (whether or not they are owned by LBS) attached to it.

Policy concerned with the examination of stored material applies to **any** computer facility provided by LBS.

3 In what circumstances can monitoring occur?

Provisions in the LBPR permit LBS to intercept and record information which can be associated with an individual's communications via LBS's services (whether made for purposes associated with LBS business or activities or otherwise). This may only be done where LBS has made reasonable efforts to inform potential users that such interceptions may be made, and in order to achieve the following aims:

- to prevent or detect crime;
- to investigate or detect unauthorized use, including the use of systems outside LBS;
- to ensure the effective and authorized operation of systems;
- to establish the existence of facts necessary to ascertain compliance with regulatory or self-regulatory procedures (e.g. harassment in breach of LBS policy), or to ascertain or demonstrate standards;
- for other lawful purposes as set out in the relevant legislation.

Stored material (including electronic mail) may also be examined for these purposes. In addition, LBS may access stored material in the event of an urgent need (see section 6).

LBS may also monitor but not record:

- received communications to determine whether they are business or personal communications.

'Authorized use' of LBS's facilities is defined in section 2 of the LBS Acceptable Use Policy. It should be noted that although reasonable personal use of facilities is permitted, excessive use that disrupts or distracts an individual from the efficient conduct of LBS business, or involves accessing or sending unlawful or offensive material (for example, obscene, discriminatory or abusive material), is prohibited; and, consequently, monitoring may take place to detect or investigate such behaviour.

Note that the law distinguishes between monitoring for operational and policy reasons. Both classes of activity must be authorized. Note that the authorization mechanisms are different for the two cases as detailed below.

3.1 Monitoring for operational reasons

LBS IT routinely monitors their systems to ensure that they are performing properly. This reflects standard good practice, and normally involves only aggregate anonymous data that does not identify individuals or the contents of their communications. IT, for example, monitors the amount of traffic flowing through parts of the LBS network.

However, a general exemption in the RIPA permits LBS to intercept certain communications where the interception is by an authorized person for purposes connected with the provision or operation of a service, for example:

- email postmasters may examine mis-addressed messages in order to redirect them as necessary, or check email subject lines for malicious code;
- system operators may monitor system traffic to determine its source, where this is necessary to ensure the effective performance of their mail servers, for example to eliminate unsolicited commercial email (UCE or 'spam');
- system and network managers may investigate which system and/or individual is the source of a denial of service attack.

The RIPA LBPR require that persons carrying out routine monitoring under this exemption must be properly authorized either through their job description or by written authorization from the appropriate person (see section 4 below).

Persons carrying out monitoring for operational reasons must be alert to the focus of their investigation changing. If, at any stage, monitoring or access to stored material is required to investigate matters of policy (or legal) compliance the appropriate authorization must be obtained as described below.

3.2 Monitoring for policy (and legal) compliance

All other activities falling under the exemptions within the LBPR will constitute monitoring for policy or (legal) compliance. Each individual act of monitoring for this purpose must be specifically authorized and documented as described in sections 4 and 5.2, respectively.

4 Who can authorize monitoring of computer or network use?

The law distinguishes between monitoring for operational and policy reasons. However, both classes of activity must be authorized. Note that authorization mechanisms are different in the two cases.

4.1 Routine monitoring for operational reasons may be authorized through staff job descriptions or by written authorization from one of the following (or their deputies) as appropriate:

- a member of the Information Security Group (in pursuance of security issues)
- a member of the IT SMT (in relation to systems under his/her authority)
- the School secretary.

4.2 Monitoring or access to stored material to investigate policy (or legal) compliance may only be carried out with written authorization from one of the following (or their deputies) as appropriate:

- the Director of Research Faculty Office or the Chief People Officer (CPO) (in pursuance of faculty/staff disciplinary matters, as appropriate)

- the Associate Dean, Degree Education and Careers Centre or the Associate Dean, Executive Education or the Associate Dean, Advancement (in pursuance of student/alumni disciplinary matters, as appropriate)
- a member of the Information Security Group (in pursuance of security issues)
- a member of the IT SMT (in relation to systems under his/her authority)
- the School Secretary.

In addition, written authorization must be obtained from Information Security **and** the LBS Data Protection Officer (DPO). Note that authorization covers an individual act of monitoring and only for the purposes and scope indicated on the authorization form.

4.3 A summary report of activities will be sent to the Chief Information Officer (CIO) for oversight purposes.

4.4 Attempts by any member of faculty/staff to implement monitoring without proper authorization will be in breach of this policy and may be the subject of disciplinary proceedings. Unauthorized monitoring may also attract civil or criminal liability.

LBS recognises that, due to the nature of computer systems, data held on its computer systems, passing across its networks, or printed out on LBS equipment, may at times be visible in readable form. In such circumstances, that data may well be viewed by LBS faculty/staff. Such incidental/inadvertent viewing will not constitute a breach of this policy, even where such viewing leads to the implementation of authorized monitoring and/or disciplinary procedures against the user concerned.

5 Procedures for monitoring computer or network use

5.1 In most circumstances where communications are to be intercepted, the RIPA and LBPR require that for the interception to be lawful, users of the service must have been informed **in advance** that interception may occur. Failure to adequately inform the users of the possibility of interception may result in their having a legitimate expectation of privacy in their communications on the service, and make the interception unlawful. This might render the material intercepted useless for the purpose of disciplinary or legal proceedings, and could render the School liable to a civil lawsuit.

The following message should be displayed wherever LBS systems are used (e.g. posters, labels on screens):

> *Communications, including personal communications, made on or through LBS's computing and telecommunications systems may be monitored or recorded to secure effective system operation and for other lawful purposes.*

Similarly, it is important to remind users of the limits on their privacy in connection with stored material. The above URL includes a reference to this policy, but in addition explicit mention of the

policy should be made in documentation given to faculty/staff or students when they are granted access to any IT facilities, or during their induction.

5.2 The application form for authorizing specific monitoring for policy (and legal) compliance (section 4.2) should document:

- the reason for monitoring, including any internal disciplinary offence or suspected or alleged civil or criminal act which may have been committed and an indication of why this is felt to be a proportionate approach;
- the scope of the monitoring;
- the intended duration;
- the names or job titles of those who will be carrying out the monitoring. A witness **must always be present**;
- steps taken to protect the privacy of the person or persons being monitored.

5.3 If there is any likelihood that an internal disciplinary offence or suspected or alleged civil or criminal act may have been committed which may result in disciplinary or legal action resulting from an investigation, specialist advice on the preservation of evidence should be sought before proceeding. LBS Information Security staff (email: infosec(at)london.edu) should be contacted in the first instance and will act as liaison with law enforcement agencies as necessary.

6 Access to stored documents (including email) for business purposes

There are occasions when LBS needs to access information held by LBS faculty/staff within electronic mail, elsewhere on their computer, or in other filestore or backup media. This will usually occur when the faculty/staff member is absent, either ill or on leave, and a situation arises which requires a rapid response. Members of LBS must be made aware that LBS reserves the right to obtain access to files held on/in equipment owned by LBS, and that the privacy of personal material stored on/in such equipment in the event of authorized access cannot be guaranteed.

Persons facilitating such access (e.g. IT staff) must **on each occasion** obtain written authorization from a person listed in section 4.2. The authorization must identify the material to be accessed, its location and why a delay in access would be detrimental to LBS's interests. If the location of the material is not precisely known the application must describe the proposed search methodology. The request must be authorized by the LBS DPO. A log of operations carried out and material accessed must be maintained and signed by the person facilitating access and a witness. A copy of this log and the completed authorization form must be given to the owner of the material.

If there is any likelihood that an internal disciplinary offence or suspected or alleged accessed. Advice on appropriate methods for carrying out this work is available from LBS Information Security.

It is intended that these arrangements are for exceptional circumstances only: applications will only be considered if they demonstrate that delay will cause disproportionate damage to LBS's interests. Normal business processes should avoid their necessity through use of role email addresses or lists, delegated access to email, appropriate file access control, etc.

Persons facilitating access must take all reasonable measures to respect privacy. However, difficulties may arise when searching for material, as there is no guaranteed method of distinguishing between business and personal items. Users are advised to minimize the risk of inadvertent viewing of private material by placing appropriate messages or files in folders (or directories) whose name includes “Personal”. (Mail filters can be set up to move messages automatically into folders according to sender or destination address, etc.)

7 Exceptional Modification of User Files

In exceptional circumstances, system administrators may need to make changes to user filestore. Examples include disabling programs which may adversely affect system or network performance, disabling software which is being used contrary to licensing arrangements or removing from public view confidential files or offensive material.

The permission of the file owner should be obtained unless the situation is of such urgency as to make this impracticable. Each filestore change and the associated justification must be logged. The file owner must be informed of the change and the justification as soon as possible.

The system administrator may not, without specific authorization from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information. If necessary, files should be moved to a secure offline archive.

8 Status of this policy

This document has been approved by LBS Management. It is subject to regular review by LBS Information Security. LBS faculty and staff are obliged to abide by this policy (and overarching Information Security Policy) as a condition of employment. Users of LBS IT services who are neither faculty nor staff are also bound by the LBS Information Security Policy.

In all cases, the act of registering as a user of LBS IT services or making use of any of the IT facilities involves implied acceptance of conditions of use and implies compliance with regulations, relevant Acts of Parliament and other relevant law.

From time to time, LBS may issue good practice guidelines and reserves the right to withdraw network services to systems or services that are not operated in accordance with those guidelines.

9 References

Relevant legislation includes:

1. The Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

2. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.legislation.gov.uk/uksi/2000/2699/contents/made

3. The Human Rights Act 1998
https://www.legislation.gov.uk/ukpga/1998/42/contents

4. The Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

5. The Employment Practices Data Protection Code Part 3 Monitoring at work
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf