Using logfiles

Privacy and Legal Issues

Any comprehensive programme of logging will capture information about the activities of individual users. In many cases this has the potential to intrude on the privacy of those individuals. Users and system administrators must be clear that the sole purpose of logfiles is to provide a better service to legitimate users, by providing computers and networks that are fit for their intended purpose and which work as reliably as possible. Article 8 of the European Convention on Human Rights states that ‘Everyone has the right to respect for his private and family life, his home and his correspondence’: all users and administrators must respect this.

Most logfiles contain personal data, so are also subject to the provisions of the Data Protection Act 1998. Users must be informed what information will be recorded and what it may be used for (as noted above, the very fact of notification may well discourage misuse of the system). Logfiles must also be protected from unauthorised access, use or modification. The Act requires that personal data should not be kept for longer than necessary; guidelines for the interpretation of ‘necessary’ are discussed in Section 2.2, on data retention, below.

The Data Protection Act allows those whose personal data is kept (“data subjects”) to request copies of information held about them. Without preparation, such Subject Access Requests (SARs) can be one of the hardest and most costly parts of the Act to comply with: however, the same processes that allow logfiles to be used to investigate problems should provide most of the apparatus required to deal with SARs.

Various Acts of Parliament make a useful distinction between traffic data and content data. Traffic data (sometimes referred to as communications data) is information about the existence of communications. For example, records that a particular user logged on to a workstation at a certain time, sent e-mails to a number of other, recorded, e-mail addresses and then logged out, would comprise traffic data about that session of use. The texts of the e-mails would, however, constitute content data. The law appears to treat traffic data as less likely to involve a breach of privacy than content: for example the rules for police access to traffic data require a lower level of authorisation than for content data.

Most logfiles will contain only traffic data. However, there are a number of electronic systems where the distinction between traffic and content data is unclear. It is considered that the subject lines of e-mail are content, rather than traffic; similarly in the case of web requests the identity of the server from which a page was requested is traffic data, whereas the rest of the URL, which may well specify exactly what the user saw, is considered to be content.

The third type of data that is essential in identifying the individuals responsible for cases of misuse is the identity of the real world individuals who own, and should be responsible for, each login account or other online identity. This information is known by ISPs (Internet Service Providers) as subscriber data, but in universities and colleges it is likely to form part of student records and staff personnel files. As information relating to an identifiable individual it is, of course, subject to the Data Protection Act.

Data Retention

Problems are rarely detected the instant they occur so, to be useful, logfiles must be kept for some period of time. However, logfiles can grow very large, so shortage of storage space may put an upper limit on what this time may be. Even if logs can be physically stored, there is little point in keeping them for so long that the quantity of information prevents convenient searching. Where logfiles contain personal data, the Data Protection Act’s Fifth Principle also requires that they not be kept for longer than necessary for the specific purpose for which they were collected. The European Directive 2002/58/EC on Privacy and Electronic Communications (amended by Directive 2009/136/EC), which applies Data Protection law to electronic communications networks, states that traffic data must be anonymised or destroyed once it is no longer required, but identifies the provision of value added services and investigation of unauthorised use as legitimate reasons to collect and retain this data. Collecting and keeping traffic data for as long as necessary to investigate misuse of computers and the network is therefore acceptable.

A number of Codes of Practice have been written in an attempt to establish a reasonable balance between usefulness of logs on the one hand and privacy and practicality on the other. Following a recognised Code of Practice should be a good defence against accusations of keeping either too few records or too many. For some time, the Code of Practice most relevant to computer and network logging has been that produced by the London Internet Exchange (LINX) in 1999, which is available online at:

https://www.linx.net/good/bcp/traceability-bcp-v1_0.html [1]

The LINX document was prepared and is maintained by members of the Exchange, who include many of the major ISPs in the UK. The document was also reviewed by the Data Protection Commissioner, responsible for ensuring compliance with the Data Protection Acts. The document recommends that traffic data should be retained for a minimum of three months to allow misuse to be traced, but that to comply with the Data Protection Act it should not be kept for more than six months except where it relates to a known case of misuse. If an investigation is in progress then data relating to it may be kept until the investigation is complete. The same minimum retention time is recommended for subscriber data. However, users of university and college computers will usually be students or staff. Both of these legal relationships involve much longer retention periods to comply with education and employment law, so information about these users’ identities will normally and legitimately be held for much longer than six months.

Following increased concern that terrorism and serious crime might be organised or committed using electronic communications, European Directive 2006/24/EC (implemented in the UK by the Data Retention (EC Directive) Regulations 2009) made it a legal requirement for public data and telephone networks to retain information about the use of their e-mail and telephony services for up to two years. However, as Janet and most of its customers’ networks are classed as private networks, these requirements do not apply. Retention of logs for these networks therefore remains a recommendation, for the purposes of network management and dealing with misuse, rather than a requirement. In particular, organisations running these networks should ensure they have a legitimate reason if they wish to keep their logs for longer than required for the investigation of normal misuse.

Data Preservation

On a small number of occasions, following major terrorist or other criminal incidents, the UK police have asked the providers of communications networks (including Janet sites) to preserve logs and other relevant files in case they contain information relevant to the investigation. The purpose of these requests is to prevent existing information from being overwritten or deleted, not to cause additional information to be collected. There is no requirement to comply, but such exercises have protected useful information for the police in the past and are considered helpful. In practice, unless the police request contains more specific instructions, the most usual response is to take a backup of main server logs and to reserve this along with a recent set of backup tapes that are not reused until the police investigation is completed.

Such data preservation is permitted, but not required, under the Data Protection Act 1998, where section 29 allows processing of data for the purposes of the prevention and detection of crime and the apprehension or prosecution of offenders. Section 28 provides similar permission where necessary for the purpose of safeguarding national security. Data preserved under either section may be exempted from the normal subject access provisions of the Act where disclosure might be harmful to the purpose.

The preserved data should be kept by the organisation in a secure place: if the police find they need access to it then they will use one of the legal mechanisms described in the next section. Organisations holding preserved data should seek periodic confirmation from the police that the information is still needed for the section 29 or section 28 purpose.

Access by Others

Evidence from logfiles may be useful to the police and other investigating authorities in cases where unlawful acts have been committed. A number of different Acts of Parliament include provisions under which such authorities may request or require such evidence to be provided to them. This section attempts to summarise the provisions likely to be encountered by universities and colleges (for that reason, provisions that only apply to public networks have been omitted). However, it does not constitute formal legal advice. The definitive source of information is the original Acts and Codes of Practice: web addresses are listed in Section 8.3. Since there may be a legal requirement to comply promptly with some of these notices, organisations should consider instituting standard procedures for responding to them. They may also wish to discuss these procedures and any requests with their lawyers.

Requirements to produce (or collect) data	• *Regulation of Investigatory Powers A* Chapter II)

	• Other Acts including: *Social Securities Fraud Act 2001* *Consumer Protection Act 1987*
Requirement to produce or give access to data	• *Police and Criminal Evidence Act 198* • *Norwich Pharmacal Orders*
Requests to produce data	• *Data Protection Act 1998*

In the case of the police or others investigating criminal offences, access to logfiles will normally be obtained by a notice under the Regulation of Investigatory Powers Act 2000. If the information sought is not communications data then a request under section 29 of the Data Protection Act 1998 will normally be used. A Production Order under Schedule 1 of the Police and Criminal Evidence Act 1984 will only be used where neither of these routes has been successful, or where the voluntary request under the Data Protection Act 1998 would not be appropriate to the investigation. Civil courts may make Norwich Pharmacal Orders if the court process requires an organisation operating a network or server to reveal the identity of one of its users.

Regulation of Investigatory Powers Act 2000

Part I Chapter II, and in particular section 22, of this Act deals with the disclosure of communications data to law enforcement and other public bodies. This came into force in January 2004 and is now the normal process for all access to communications data, replacing section 29(3) of the Data Protection Act 1998.

Communications data is information about traffic on a network, but not the contents of that traffic. Section 21(4) of the Act provides a full definition of Communications Data, separating it into three types:

> (a) Information forming part of a communication, that is needed by the system to deliver the communication from its source to its destination. For example, source and destination addresses and routing information.
>
> (b) Other information concerning the use of the system by individual users. For example, times when individual users were logged on and the IP addresses they were allocated.
>
> (c) Other information about the users of the system, referred to elsewhere as subscriber data. For example, the identity of the owner of a login name or e-mail address.

Logfiles may contain any or all of these types of communications data. Some logfiles will also contain information that is not communications data such as the subject lines of e-mails or full URLs of web requests (only the identity of the web server is communications data), which must not be disclosed under section 22. Responding to a section 22 notice may therefore require making edited versions of logfiles with these unauthorised types of information removed.

The Act permits any designated authority to issue a notice to a communications provider requiring either that existing communications data be disclosed or that particular communications data be collected. Communications providers are widely defined (not only public networks are covered) and would certainly include any university or college providing Internet access to its members. A provider receiving such a notice must act on it, otherwise it may itself be committing an offence. The Regulation of Investigatory Powers Act makes the authority that issues a notice responsible for ensuring that it is proportionate: the communications provider releasing the information is not required, or entitled, to make any judgement on this. The purposes for which a notice can be served include interests of national security, detecting crime and preventing crime or disorder, national economic wellbeing, public safety, protection of public health, assessment of taxes and duties, preventing death, and preventing or mitigating injury to an individual's physical or mental health.

To be allowed to issue notices under section 22, an authority must be designated by the Home Secretary. The initial list of authorities was published as The Regulation of Investigatory Powers (Communications Data) Order 2003 (Statutory Instrument 2003 No. 3172). To the law enforcement authorities included in the Act (listed in Schedule 1 of the Regulations) this adds the emergency services, central and local government departments, the NHS and others with powers to investigate compliance with particular laws (listed in Schedules 2 and 3). Many of these authorities do not have powers to access the whole range of communications data set out in section 21(4) and above – many are limited to the subscriber data of type (c) and some are restricted to particular types of communication services – and in some cases a more senior officer is required to authorise notices for the more intrusive types of data. The Schedules to the Regulations set out these arrangements in detail.

For some time, police forces have had designated Single Points of Contact (SPoCs) for dealing with the communications industry. Officers staffing the SPoCs have been specifically trained both in the legal requirements of handling data and in what is likely to be practical for network operators to provide. SPoCs have been useful to ensure that the law is used properly and that the evidence obtained is suitable for the investigation and subsequent prosecution. The Home Office has therefore granted the new authorities powers under section 22 to ensure that their staff have equivalent training and work in a similar way as the police SPoCs. The Home Office is maintaining a register of individuals designated to exercise the powers on behalf of each authority, and every section 22 notice must be approved by one of these designated persons before it is served on a communications provider.

The process of issuing notices is described by a Code of Practice. A standard form requiring disclosure of communications data has been published and should be used for all notices. Notices that are received by Janet sites should be checked to confirm that they come from a designated authority, request data which that authority is entitled to receive, and have been issued by the appropriate designated person or SPoC. Janet CSIRT has access to the Home Office register and can confirm that notices have been approved by the correct designated person. Notices that appear incorrect should not be acted upon. There have been reports that individuals have attempted in the past to use other statutory powers (see next section) to gain access to information they did not have authority to see and the Home Office has asked for reports of any attempts to abuse the section 22 powers in this way.

It is strongly recommended that any organisation likely to receive statutory notices under the

Regulation of Investigatory Powers Act 2000 or other statutes (see below) should designate and train a person or office to deal with the notices, and that all enquiries regarding notices should be directed to that person or office. Legal advice is likely to be helpful when setting up these procedures.

Other Statutory Notices

The Regulation of Investigatory Powers Act 2000 (RIPA) is just one of a number of pieces of legislation that create rights for designated authorities to obtain information for particular purposes. These include the Consumer Protection Act 1987 (trading standards) and the Social Security Fraud Act 2001 (benefits agency), as well as court orders and police warrants. The Home Office intends that all access to communications data will eventually be done under RIPA powers: however, it is likely to be some time before the other powers stop being used.

When presented with a valid statutory notice by a person entitled to issue that notice, it will normally be an offence not to provide the required information. However, anyone receiving such a notice must check both that the notice is valid and that the person is entitled to use it. This will normally involve checks with appropriate third parties.

The LINX has published a Best Current Practice document on privacy, which contains useful guidelines on dealing with statutory notices. This is available at:

https://www.linx.net/good/bcp/privacy-bcp-v1_0.html [2]

Court Orders

Schedule 1 of the Police and Criminal Evidence Act 1984 (PACE) enables a police constable to ask a judge to make an order requiring a person to either produce or give the constable access to information that the person holds or has access to. An order will only be granted if there are reasonable grounds for believing that the information will be of substantial value in investigating a serious offence, and could be used as evidence. Furthermore all other means of obtaining the material must have either been tried or found inappropriate. The judge will then decide whether it is in the public interest to make the order that the information be produced.

A production order may be served on an individual, a partnership or corporate body, and may be delivered either by hand or post. The person or body on whom the order is served must then either produce the information, or give access to it, within a fixed period, typically seven days from the issue of the order. Failing to comply with an order, or tampering with the information once the order has been served, is a contempt of court: a serious criminal offence.

PACE production orders are used as a last resort, generally where information is not accessible by any other power. They may also be used in place of Data Protection Act 1998 requests (see below) in cases where it is desirable to have a judge rule on the proportionality of disclosure before it occurs, rather than after as is the case with the Data Protection Act process. PACE production orders should be simple to deal with: the recipient must comply with the order or commit a serious criminal offence.

PACE orders, RIPA notices and DPA requests all apply only to criminal offences. For civil cases a more limited order was created following the case of Norwich Pharmacal Co. v Customs and Excise Commissioners [1974] AC 133, and therefore known as a Norwich Pharmacal Order. These may be issued by a court where there is evidence that a civil wrong (such as defamation or copyright breach) has been committed but the identity of the wrongdoer is not known to the victim. Online, the victim will often only know a nickname, e-mail address or IP address for the wrongdoer. If the court considers that a third party (for example a network provider) is able to reveal the real-world identity of the person associated with this information then the court may order the third party to do so. The victim can then begin a civil case against that person. As with PACE production orders, Norwich Pharmacal orders should be simple to deal with: the recipient must either disclose the identity as ordered by the court or explain that they are unable to determine it.

Data Protection Act 1998

Various sections of the Data Protection Act permit data controllers to disclose personal data without breaching their obligations under the Act. In particular section 29(3) permits this where the information is required for the prevention, detection or prosecution of crime, and section 28 applies where the disclosure is required in the interests of national security. In all cases, disclosure is voluntary and the data controller must consider whether the breach of privacy is proportionate to the stated reason of why the information is needed. The Information Commissioner has a useful guide to how to make this decision at

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/section_29_
[3]

Although these provisions are still in force, they have been superseded for communications data by the powers under the Regulation of Investigatory Powers Act described previously and should no longer be used for this type of information. Where other types of information are concerned, the request for disclosure should be made in writing on a standard form, giving enough information about the purpose for the assessment of proportionality to be made. In the case of a request from the police, this form should always be authorised by the force's Single Point of Contact (see above).

As discussed in the previous section, a PACE production order may be preferable in some circumstances to a Data Protection Act request as it allows this assessment of proportionality to be made by a judge rather than the recipient of the request.

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/using-logfiles

Links
[1] https://www.linx.net/good/bcp/traceability-bcp-v1_0.html
[2] https://www.linx.net/good/bcp/privacy-bcp-v1_0.html
[3]
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/section_29_gpn_v1.pdf