



Computers and the Law

Most people who work with computers will have at least heard of the Computer Misuse Act and the Data Protection Act: from their titles alone it is clear that these apply to computers. However there are a number of other, less obvious, Acts of Parliament (see below) which may well apply to you, especially if you have anything to do with systems administration. While none of them can be recommended as light reading, it is worth having some idea of how they may affect you.

Of course there are also a very large number of "real world" crimes that can be committed with the assistance of a computer. These range from defamation and violation of copyright through blackmail and harassment to pornography. Contrary to popular opinion the Internet is not "lawless" and the fact that an offence is committed through electronic means does not make it any less of an offence, nor is it likely to mitigate the punishment.

HMSO publishes all public Acts of Parliament passed since 1988, and some other related Acts, on its web site at: <http://www.legislation.hmsso.gov.uk/acts.htm>

Definitive copies of all Acts can be purchased as paper documents from HMSO or their agents, and may also be available in libraries.

The JISC have published briefing papers on a number of legal issues at: <http://www.jisc.ac.uk/pub/index.html#briefing>

Their legal information service is at: <http://www.jisc.ac.uk/legal/>

We recommend that organisations should establish contact with their local police force before they have problems. Such relationships can be highly beneficial to both sides. Many police forces now have designated officers who specialise in computer crime. If you do not know who to talk to in your area, ask the JANET-CERT, who has contacts in several forces and may therefore be able to help.

Regulation of Investigatory Powers Act 2000

This Act defines rules for interception of traffic on all postal and telecommunications networks. It applies to all users and operators of networks, whether local or wide area, and to any action which may cause the content of a message to become known to people other than the sender and recipient. The Act and its supporting regulations only authorise certain groups to examine traffic on networks and restrict the purposes for which monitoring and recording can be used.

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

Monitoring for business purposes, such as ensuring compliance with acceptable use policies, is covered by a separate statutory instrument.

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

Data Protection Act 1998

This Act and related European Union legislation place controls on the processing and use of personal information. The 1998 Act, which came into force in March 2000, protects all personal data whether held in electronic or manual filing systems. Further information is on the Registrar's website:

<http://www.dataprotection.gov.uk/>

Computer Misuse Act 1990

This Act deals with unauthorised access to, or modification of, computer material. Its scope is remarkably wide, including almost any attempt to modify or impair the function or reliability of any computer, program or data without authority to do so. The offender must be aware at the time that their action is unauthorised; for this reason it is recommended that login and other banners be displayed wherever possible.

http://www.legislation.hmsso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Telecommunications Act 1984

Section 43 of this Act concerns "improper use of public telecommunication systems". It makes it an offence to send untrue messages intended to cause annoyance, inconvenience or needless anxiety; also messages that are obscene or grossly offensive. Not only do such messages contravene the acceptable use policy of most computer networks (including JANET), they may also be criminal.

International Law

A survey of European Law is being developed at <http://www.eurocert.net/legislature.html>

Please note that this article is written with no legal expertise and that no-one should take any action based solely on its content. In particular, readers outside England and Wales may be subject to different legal systems.