67th IFLA Council and General Conference
August 16-25, 2001

Code Number:	**172-83-E**
Division Number:	**0**
Professional Group:	**Committee on Copyright and other Legal Matters**
Joint Meeting with:	**-**
Meeting Number:	83
Simultaneous Interpretation:	**Yes**

Privacy and information technology or what a give away!

Sue Brown
Chair of the UK Copyright and Indexing Group
UK

Introduction

“Privacy” and “Information Technology” – we seem to live in a world where possession and control of these are both highly valued in their own right and something that we desire more and more of – more privacy to do our own thing and be ourselves – more information technology to live, learn and work more quickly and more efficiently. In this context it could be said to be a perception that Information Technology makes it easier to be more private – information, delivered by technology just for me. However there are conflicts of interest between the desire for privacy and the use of IT to provide information which no one set of rules can fully resolve.

The sophistication of today’s IT makes it so easy and painless to collect data about us and our activities that if used without “due care and attention”, it threatens to invade our privacy. What will tomorrow’s IT bring? We give information about ourselves when undertaking so many transactions. When we open a bank account, make an appointment to see a doctor, order a book, or buy an airline ticket, register for a library card, or sign up to receive an electronic journal. We say where we live, who with, how much we earn, what we like to buy, read, where we visit … The list is endless. And the potential for misuse of that information grows daily.

Information given once can be used many times and in many combinations with the use of new technology. The implications of control to avoid misuse are a challenge to us all both as data subjects, the person to whom data refers, and as data controllers, any person or body determining the purposes and the means of the processing of data. As librarians we have to consider the conflicts between privacy, the potential for abuse of IT systems and the effective and efficient delivery of free access to information.

I have been asked to look at some of the issues relating to privacy and the responsibilities of libraries, highlighting in particular the European Directive on Data Protection and the possible impact on privacy of Electronic Copyright Management Systems (ECMS).

What I hope to achieve in this presentation is to impart some knowledge by outlining some of the European legislation, obviously from a UK perspective, raise some of the conflicts between Privacy and the use of IT and to make you think how you might wish to deal with them in both your private and your work life. One thing is certain, to do our jobs effectively in the future we have to know about the issues.

Data protection in Europe

The development of a frontier-free Internal Market and of the so called "information society" will increase the cross-frontier flows of personal data between Member States of the EU. In order to remove potential obstacles to such flows whilst maintaining a high level of protection within the EU, it was necessary to harmonise data protection legislation. The European Commission also engages in dialogues with non-EU countries in order to ensure a high level of protection when exporting personal data to those countries. And it initiates studies on the development on European as well as international levels on the state of data protection.

The EU legislation also came about because although national laws on data protection aimed to guarantee the same rights, some differences existed. These differences could create potential obstacles to the free flow of information and additional burdens for economic operators and citizens. Some of these were: the need to register or be authorised to process data by supervisory authorities in several Member States, the need to comply with different standards and the possibility to be restricted from transferring data to other Members States of the EU. At the same time some Member States did not have any laws on data protection.

So, just to repeat, the harmonisation of data protection rules in the EU aims to achieve the free movement of information, including personal data, between Member States whilst at the same time ensuring a high level of protection for any person concerned. The resulting legal framework is found mainly in Directive 95/46/EC ("the Data Protection Directive"), adopted on 24 October 1995, dealing with the protection of individuals in the processing of personal data and the free movement of such data. Member States were required to give effect to the Directive within three years of its adoption, i.e. by October, 1998.

European Legislation

European Directive on Data Protection 95/46/EC – 1995.
Harmonisation of EU Directive amongst EU Member States – 1998.
UK Data Protection Act 1998.

European Directive on Privacy in Telecommunications 97/66/EC.
European Convention on Human Rights.
UK Human Rights Act 1998.
European Directive on Copyright 2001.

The Data Protection Directive applies to 'any operation or set of operations which is performed upon personal data,' called 'processing' of data. Such operations include the collection of personal data, its storage, disclosure, etc. and personal data is anything that can identify you as an individual. The Directive applies to data processed by "automated means" e.g. a computer database of customers, and to data that are part of or intended to be part of non automated 'filing systems' in which they are accessible according to specific criteria. For example, the traditional paper files, such as a card file with details of clients ordered according to the alphabetic order of the names. It is format or carrier neutral.

The Data Protection Directive does not apply however to data processed by individuals for purely personal reasons or household activities (e.g. an electronic personal diary or a file with details of family and friends). It also does not apply to areas such as public security, defence or criminal law enforcement, which are outside the competence of the EC and remain a national prerogative. National legislation generally provides protection for individuals in these areas.

So when it is a matter of “National Security” or criminal law enforcement what protection does the individual really have about the use and access to personal data held about them? Not very much is the answer. What are your thoughts on the following? As librarians in charge of large, easy to access data files about people’s reading habits or whereabouts, when it is a matter of national security where do our responsibilities lie? Monitoring of any use of the internet by individuals in libraries will produce further dilemma. For example, yes that person did take out a book on fertilisers and its alternative uses on a particular date. Did they then go on to put that knowledge to illegal use? What should you do?

What can you do? What can you not do? When examination of an issue system might prove one way or another where an individual might have been. These are serious things for us to think about and to consider the long term effect on our relationship with our users.

The data protection legislation has 8 aims listed as principles.
The Data Protection Principles

1. **Personal data shall be processed fairly and lawfully.**
   Regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

2. **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**
   Regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

4. **Personal data shall be accurate and, where necessary, kept up to date.**

5. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**

6. **Personal data shall be processed in accordance with the rights of data subjects under this Act.**

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

   Having regard to the state of technological development and the cost of implementing any measure, the measures must ensure a level of security appropriate to-

   (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
   (b) the nature of the data to be protected

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Issues for Librarians and Information Workers

I see the issues as the conflicts of interest that may arise between the rights of privacy of individuals – Data Protection, the need to control the IT applications delivering services using personal data about individuals – management of technical processes and the desire to make use of all that information – Freedom of Access to Information.

Where are some of these conflicts, some have been mentioned previously, and what are our responsibilities as Librarians? Certainly conflicts arise in the following areas:-

a) Use of personal data held in Membership Files
b) Provision of access to the Internet
c) Copyright

Membership Files

Under Data Protection Principles librarians need to be aware of:-

- the purposes for which personal data is held
- that it is adequate, relevant and not excessive
- that it needs to be accurate and updated regularly
- that it should not be kept for longer than is necessary
- that appropriate technical and organisational measures should be taken to stop unauthorised processing, accidental loss etc. or damage to data.

In our role of providing access to information we may want to offer "tailored" services to users, especially in the workplace and academic library sectors. We live in a world where we are constantly having to justify our existence and provide figures to support it. We want to ensure that we provide what users want and that they use our services rather than those of someone else. So we might want to provide for example, alerting services to users who like to read a particular type of fiction or certain authors – if you like this then you may like that, students studying certain topics and researchers, etc. Amazon.Co highlight products similar to those of your last order when you next access their database. The technology is there, this is an easy number crunching exercise matching two different types of data – you the individual with the items you have borrowed. Store cards exist to keep information on our purchasing habits to anticipate and tempt future business, not for the customer's convenience.

But when does this become an invasion of privacy? Is it when the "mail shot" becomes too invasive by providing too many alerts, when the topics extend to facts that we had not considered, e.g. connected to an item borrowed, but actually not found to be appropriate or are about a topic that really is no one else's business? When are we as the third party possessors of this information placed in a dilemma because of our knowledge of that information? Is it when records show a trend in information gathering on Euthanasia by someone in their 70s, or on child abuse by a 16 year old? When does this become a paid for service that individuals who can afford to, buy into? Rich student versus poor student?

Internet Access

As librarians I think it can be said that we are committed to the widest possible freedom in the dissemination of information. In the UK, Government has a policy of providing access to the Internet in every Public Library that is free of charge at the point of access. The aim of the Government policy is to lessen the divide between the Information Rich and the Information Poor. In the UK we have no general right of access to information and Data Protection is closely linked to Freedom of Access to Information. Consequently, the role of the library and information service is essential to enable individuals to enjoy comprehensive access to the widest range of information.

As I have just said, traditionally there have been no constitutionally protected rights guaranteeing freedom of access to information, a right to freedom of speech for example. However the Human Rights Act 1998 has incorporated the European Convention on Human Rights into domestic law. From 2 October 2000, every British citizen can take any organisation to a British court for breaching their rights. In particular, the right to privacy (Article 8) is considered to be one of the most sensitive areas – every citizen has the right to protection of family and private life. This has to be balanced against a right to freedom of expression (Article 10). Library and information services therefore need to be informed about their responsibilities under this legislation and be aware that their policies may be subject to challenge.

Library and information services may decide to monitor Internet use to help them ensure or prove that they are fulfilling their legal and other obligations. Monitoring may help to enforce policy and act as a deterrent to inappropriate or illegal use. But any use of monitoring systems has to be made clear to users. Again, the library and information service will need to ensure that its monitoring is not inconsistent with its legal obligation under Data Protection legislation and other safeguards of user confidentiality and privacy. What personal data needs to be collected for monitoring purposes and would this invade an individual's privacy?

Before providing Internet access and services for users, library and information services should have clear policy statements and guidelines in place. Such policies should make clear the duties and responsibilities of users (they have them too!) by reminding them, for example, of their legal obligations and stating what constitutes acceptable use and behaviour in a library setting. However, libraries need to take care that their policy on acceptable use does not unnecessarily or unintentionally restrict the legitimate needs and interests of their users.

The issues around the use of filtering software are complex and contentious. A desire to protect children from exposure to illegal or harmful material when using the Internet may conflict with the right of privacy that an adult may expect to access material that is legal and not harmful to them. Under their Code of Professional Conduct all members of the UK Library Association are obliged to "facilitate the flow of information and ideas, and to protect and promote the rights of every individual to have free and equal access to sources of information without discrimination and within the limits of the law". (One to think about if we had more time!)

EMAIL

Also with the provision of access to the Internet comes the thorny problem of Email! As more and more information business is carried out digitally this is just as much an "employment" issue for librarians as managers as it is as part of Internet access for individuals. As both employer and employee you need to know about the following:-

Instant communication with a global audience and at almost no cost has made e-mail an essential tool for business. But the ability to send messages around the world at the touch of a button has brought its own problems. These include:- attracting negative publicity, increasing employers' liability to actions for defamation, racial or sexual harassment and increasing the potential for employees unintentionally to create contractual commitments for which their employers may be responsible.

In the UK some complex pieces of legislation inter relate. The Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA) are the main pieces of legislation governing interception and monitoring of e-mail. RIPA establishes the principle that communications must not be

intercepted without consent. And as a general rule, providing that the lawful interception of communications over public networks or private networks linked to the public network, should be based on the consent of both the sender and the intended recipient of the e-mail.
But the Secretary of State has powers of exception. They both provide for criminal and civil liability.

So, regulations made under RIPA set out the general circumstances under which monitoring and interception are permitted, while the Data Protection Act, regulating the use of personal data, determines whether or not monitoring or interception can lawfully take place where it involves the processing of personal data.

Then the Human Rights Act 1998 guarantees rights of privacy and Public authorities may not act in a way incompatible with an individual's right to have respected private and family life, home and correspondence.

So, organisations can monitor – but not record – communications to establish whether e-mail is relevant to their business. But they must make reasonable efforts to inform every person who may use the e-mail system that their communications may be intercepted.

With employees, this may be done through e-mail policies set out in staff handbooks, compliance with which should be based in the employment contract. For all third parties (recipients), a statement automatically printed on the bottom of each outgoing e-mail is recommended. Sometimes the disclaimers are longer than the email! Employers should also make known to their employees the consequences of breaching the e-mail policy and ensure that the policy is enforced whenever breaches come to their attention.

Copyright

With the provision of electronic document delivery comes the conflict between access and copyright considerations – media copyrights, author rights, access control and payment for digital multimedia material. The sophistication of the technology which enables almost instant delivery of documents, as they say anytime, any place, anywhere, is being utilised to provide an effective solution adding extra protection to Copyright laws. The EU Directive on Copyright became law in June 2001 and this time Member States have only 18 months to incorporate the Directive into National legislation.

The widespread use of electronic technology to produce, store, manipulate and distribute information of all kinds and the arrival of digital technologies for handling text, sound and visual images has opened up many possibilities for use but poses serious questions about copyright. The different players involved (authors, publishers, distributors, intermediaries and users) all have different, yet interdependent, requirements of the copyright system. A balance needs to be maintained between the different interests. The implementation of Electronic Copyright Management Systems (ECMS) can go some way to achieving a balance although even these cannot achieve total control and an element of trust is always needed.

Electronic Copyright Management Systems are technical solutions such as encryption, tagging, digital fingerprinting, data identifiers, watermarks. What they do is track and control the movement of works in digital forms. Ultimately they can prevent unauthorised access to prevent piracy etc. But in order to achieve this, personal data must be given in return. So a document, barcode or watermark information is supplied with an encryption stating that it is supplied by "x" organisation to "y" person giving their name, address, date, and saying whether payment has been made, "copyright cleared with royalty paid".

The technology is sophisticated enough to track use and identify users, and for librarians ECMS will mean setting up systems to track and record document usage, mechanisms for charging, mechanisms for access control, clearance requests and overall copyright management. All of which will cost money and create the potential for misuse.

An example of a European Developed ECMS system is
CopySmart (a software and PC-card with a smart card reader to be inserted into a PCMCIA connector)

The consortium, named CopySmart, initiated by the French smart card manufacturer Gemplus includes Euritis (France), Phoenix Technologies Ltd. (UK), British Library (UK), Bureau van Dijk (Belgium) and the Open University of the Netherlands.

CopySmart is conceived for publishers, fee collecting companies, licensing agencies, distributors, libraries and universities which give access to end users to any type of electronic documents: basic objects (image, sound, text) and complex objects (applications, data bases, multimedia works …) in an off-line (e.g. CD-ROM) or on-line (e.g. Internet) environment.

Implementation of legal clauses registered together with authors and publishers, gives a controlled access to any digital information in "a completely trusted" environment. But in order to participate as a TTP – Trusted Third Party, or to negotiate permission to carry out an exception you have to identify yourself, i.e. hand over personal data. It's a big element of trust!

Others systems include:-
COPICAT
CITED
COPEARMS
IMPRIMATUR

In most cases existing laws and practices provide an adequate framework for the development of Electronic Copyright Management Systems. Eventually an ECMS may be capable of assisting in the identification of copyright owners, the acquisition of any acquired rights and permissions, the application for registration of claims to copyright and the recording of copyright documentation with the Copyright Office, and the collection of royalty payments.

Conclusions

For librarians the "digital revolution" is double-edged. It offers opportunities, almost on a daily basis, to improve information services by faster delivery, more efficient retrieval and solves "basement storage" problems overnight! But it also leads us to question the responsibilities that librarians have as gate keepers to the riches of that revolution. We have an expectation that new technology will be used to improve services for the good of society. The problems start when we acknowledge that those controlling the new technology and the data it can hoard may not be so scrupulous. Legislation set up to combat the unscrupulous then causes further dilemma.

The conflicts and issues bought about by the desire to protect our privacy and at the same time maximise the use of technology are something we have to keep talking about. As a profession we have to show that we are responsible in the delivery of our services, that we are aware of the rules and regulations and that we are willing and able to educate users about the issues. The access that new technology gives us to information has a price – it is the give away of personal data and it will drastically change our relationships with users. What I hope this presentation has done is to raise your awareness of the issues and the importance of your contribution to the debate.