Date : 13/06/2008

Ethical, Legal and Political Dimensions of Managing Personal Information: A Discussion Paper.

Dr. J. Eric Davies
Honorary Visiting Research Fellow
Department of Information Science,
Loughborough University. Loughborough. LE11 3TU.
UK.
Email: j.e.davies@lboro.ac.uk

Meeting: **165 Government Libraries**
Simultaneous Interpretation: Not available

WORLD LIBRARY AND INFORMATION CONGRESS: 74TH IFLA GENERAL CONFERENCE AND COUNCIL
10-14 August 2008, Québec, Canada
http://www.ifla.org/IV/ifla74/index.htm

Introduction

The management of personal information presents many challenges in modern society: ethical, legal and political. The need to respect information about people has been recognised in many legislatures and is embedded in international treaties. This paper discusses some of the general issues raised and focuses upon privacy in particular. It draws generally, but not exclusively, on United Kingdom and European Union approaches. A delicate balance exists between the right to individual privacy and the needs of knowledge-based societies to perform successfully in terms of policy and practice. Identifying the fulcrum of this balance is no mere philosophical exercise. It has important implications for the way in which government and business are conducted, and in how people perceive the society in which they live. Library and information managers are not immune from the challenges presented by these issues and service delivery has to be matched with appropriate regard for personal privacy. How the individual as citizen (including as a user of library and information services) fares in this information universe is the underlying theme that permeates this paper.

An anatomy of privacy

Whenever, and wherever the ethical management of personal information is considered, the concept of privacy will be encountered as a key factor that determines the dimensions of the boundaries of activity, both politically and practically. But what exactly is privacy; and to what extent does it exist in free societies as a right?

The *Oxford English Dictionary* defines 'privacy' as:

> … the state or condition of being alone, undisturbed, or free from public attention, as a mater of choice or right; freedom from interference or intrusion.

The idea of personal privacy as something to be enjoyed, nurtured and indeed protected, prevails in many cultures and contexts and it finds support in international

fora. The United Nations *Universal Declaration of Human Rights*[1] asserts, in its Article 12, a universal entitlement to privacy:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks**.**

Similarly, the *European Convention on for the Protection of Human Rights*[2] from the Council of Europe proclaims that:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

It goes almost without saying that, in the interests of gender equality, we should understand 'his' to mean 'hers' as well in both these texts.

It has not always been easy to legislate to protect privacy. It is sometimes difficult to achieve consensus on the nature and extent of protection desirable. Over thirty-five years ago, in the United Kingdom, the Younger Committee on privacy noted in its report[3]:

> The concept of privacy causes little difficulty to the ordinary citizen. He can readily identify the part of his life which he considers to be peculiarly his own and for which he claims the right to be free from outside interference or unwanted publicity. Nevertheless, the kinds of privacy to which importance is attached and the intrusions against which protection is sought differ so widely from one individual to another and from one category to the next that it has not so far been found easy to fit the concept tidily into a single legal framework, so as to give it reasonably comprehensive recognition and protection through the civil and criminal law.

Privacy may be protected through related legislation regarding trespass or breach of confidentiality, and some countries have specific privacy laws. Both the United States of America[4] and Canada[5], for example, have legislation that underpins privacy with respect to personal information held by government institutions. Privacy also features in the semi- formal, yet generally effective, arrangements such as those of the United Kingdom's Press Complaints Commission[6] which seeks to function as a safeguard against excessive press and media intrusion into people's lives.

While it remains undisputed that arbitrary and unfair infringement of a person's privacy has to be condemned, it has become increasingly difficult for a person to maintain a life of complete secrecy and be a fully participating member of society especially in the 21st Century. The mechanics of living in a modern society, and in particular a knowledge-based society, entail a degree of information sharing if it is to

---

[1] UNITED NATIONS. *Universal Declaration of Human Rights.[Article 12]*. New York, U.N., 1948.
[2] COUNCIL of EUROPE. *European Convention for the Protection of Human Rights and Fundamental Freedoms.[Article 8; Section 1]*. Strasbourg, Council of Europe, 1950.
[3] GREAT BRITAIN. Committee on Privacy. *Report…* London, HMSO, 1972. (Command Paper: Cmnd 5012) (Chairman: Kenneth Younger)
[4] UNITED STATES Laws, Statutes. *Privacy Act.* 1974 (as amended)
http://opm.gov/feddata/USC552a.txt
[5] CANADA. Laws, Statutes. *Privacy Act.* 1985 (as amended)
http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-21///en
[6] PRESS COMPLAINTS COMMISSION. *Editors Code of Practice*. London, PCC, 2007.
http://www.pcc.org.uk/assets/111/Code_Aug_2007.pdf

function at all effectively. In short, there is a general requirement for appropriate and adequate information to be available to enable a society to function. A balance has often to be struck, therefore, between the right to privacy and the need, by a range of agencies, to know. It follows that if people are to maintain confidence in organisations and their systems, safeguards are required against the misuse of that need to know and the personal information that accompanies it. There is, moreover, an imperative for transparency in what agencies do with personal information. At the same time, individuals have to be aware of the risks, as well as the advantages, of sharing personal information. Recent reports[7] [8]regarding social networking sites, for example, suggest an alarming indifference to, or at best unawareness of, the risks by some people.

Technology and privacy

Technology has added, and continues to add, new dimensions to the ways in which personal information may be gathered, stored and used. It has also brought into sharper focus the ethical, legal and political features of such activity.

Over three decades ago, there was already widespread concern regarding the power and potential of mass data processing to infringe upon personal privacy and damage a person's interests. A document from the United Kingdom Government, which appeared in 1975, neatly summarised prevailing concerns:

> What is special about computers?
>
> None of the functions carried out by computers within information systems is different in kind from those which are, or could in principle be carried out by traditional methods. But there are important differences in the way, and the speed at which those functions can be performed by computer systems on the one hand, and by traditional systems on the other.
> The speed of computers, their capacity to store, combine, retrieve and transfer data, their flexibility and the low unit cost of the work which they can do have the following practical implications for privacy:
> (1) they facilitate the maintenance of extensive record systems and the retention of data in those systems;
> (2) they can make data easily and quickly accessible from many distant points;
> (3) they make it possible for data to be transferred quickly from one information system to another;
> (4) they make it possible for data to be combined in ways which might not otherwise be practicable;
> (5) because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the records, or what is happening to them. [9]

The technology of the 21st Century extends far beyond what was envisaged in 1975. To begin with, the availability and power of information technology have increased dramatically, so that in the developed world personal ownership of computers and

---

[7] Davies, G. *Data Protection Topline Report*. Wilmslow, Information Commissioner's Office, 2007. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/research_results_topline_report.pdf

[8] New front in the battle against identity theft. *The Independent.* 23 November 2007.

[9] GREAT BRITAIN. Home Office. *Computers and Privacy*. London, HMSO, 1975. (Command Paper: Cmnd. 6353)

access to networks is almost a commonplace. The internet allows data to be moved around the globe at the speed of light and it enables widely separated systems to be linked to create a pervasive computing environment.

The laptop computer with wireless networking confers a remarkable portability on data storage, processing and connectivity. The mobile telephone has become almost universal and, with it, the concept of sharing and exchanging not only the spoken word, but also images and text.

In addition, data capture technology now extends to the breadth of satellite imaging on the one hand, to the depth of iris identification on the other. The data gathered embraces real time images and sounds from the street, DNA profiles and voicemail, as well as conventional text and facts. Moreover, the remarkable increase in both storage capacities and processing capability combine to raise the potential for data mining to new dimensions. The trend is discussed and illustrated in a recent book by Ayres.[10] The often quoted Moore's Law which describes the power of microprocessors as doubling every two years is matched by an equally significant and spectacular phenomenon regarding data storage densities. Kryder's Law postulates that the growth of storage capacity of hard drives doubles every two years; and furthermore, the cost per gigabyte also declines.[11] Both have considerable implications for the capacity to extract new meaning from information of all kinds, including personal data.

Attitudes and habits have also evolved regarding the use of personal information and information technology, perhaps through indifference or unawareness of the implications of so readily disclosing information. As was noted earlier, social networking internet sites foster the disclosure and exchange of personal information and test the boundaries of privacy in new ways. As online transactions in government, banking and commerce grow, individuals volunteer yet more information about themselves. Millions of consumers daily and, it would appear willingly, provide a range of information regarding personal spending through supermarket loyalty cards which offer mild inducements in return. The result is that an ambivalence to privacy appears to be developing with some information being freely volunteered, while at the same time there is a concern regarding what is known about individuals and how it is used. Another symptom of concern regarding privacy, it may be argued, is the number of paper shredders that are now sold for home use.

All of these factors contrive to create new challenges to the use of personal information. Lest however, technology be pilloried too emphatically, it is salutary to observe Michael Gorman's wisdom in his book: *Our Enduring Values: Librarianship in the 21st Century*:

> The point is that it is not technology that is the enemy of privacy but our joyful use of technology. [12]

Safeguarding personal information.

---

[10] Ayres, Ian. *Supercrunchers: How anything can be predicted*. London, John Murray, 2007.
[11] Walter, C. Kryder's Law. *Scientific American.* 293 (2) July 2005. pp. 32-33.
[12] Gorman, Michael. *Our Enduring Values: Librarianship in the 21st Century*. Chicago, American Library Association, 2000. (Chapter 10 - Privacy. pp.144 – 157.)

The most effective means of ensuring fair treatment of personal information is the creation of a regime in which there is openness and transparency regarding what is being done, and one that renders the use of information open to challenge. Such an approach needs to be underpinned by legislation to ensure that it is effective. Many nations now have legislation and mechanisms in place to ensure that personal information is treated responsibly by both the public and private sector. This does not only entail respecting individual privacy, but also ensuring that data is reliable, and is used fairly.

The earliest example of data protection law is credited to the Lander of Hesse in Germany in 1970. Subsequently, many nations adopted legislation. Both the Council of Europe and the Organisation for Economic Co-operation and Development were instrumental in encouraging the adoption of data protection measures by individual states. The former through a treaty[13] opened for signature in 1981, and the latter with a set of *Guidelines*[14] published in the same year. Their interest reflects the trading implications of efficient transborder data flow in a global knowledge-economy as well as the protection of individual privacy. The need to harmonise the various measures being applied within member states led to the European Union[15] to issue a *Directive* in 1995, which served as a benchmark for legislation. Its objectives, as documented in Article 1, are concerned with the free flow of data between member states as well as with the fundamental rights and freedoms of individuals:

> Article 1 Object of the Directive:
> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

The *Directive* forms the basis of current data protection legislation in the United Kingdom, which was enacted in 1998. The Data Protection Act[16] is described in its preamble as:

> An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

The Act specifies acceptable activity and installs a system for monitoring and regulating the use of personal data. It pertains to personal data in any form: analogue, digital, print, images and audio. Acceptable activity is specified through a series of

---

[13] COUNCIL OF EUROPE. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg, Council of Europe, 1981.
(European Treaty Series No. 108)

[14] ORGANISATION for ECONOMIC CO-OPERATION and DEVELOPMENT.
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
Paris, OECD, 1981.

[15] EUROPEAN UNION. *Directive 95/46/EC of the European Parliament and of the Council of 24th Oct. 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data.* Brussels, E.U., 1995. (In: Official Journal of the E.U. Part (L), 23rd Nov. 1995, p.31).

[16] GREAT BRITAIN.Laws, Statutes. *The Data Protection Act.* (Public General Acts 1998 - Chapter 29). London, SO, 1998.

general principles to be followed in activities involving personal data. Briefly summarised, they require personal data to be:

- processed fairly and lawfully
- obtained and processed only for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date.
- not be kept for longer than is necessary
- processed in accordance with the rights of those who are subjects of the data
- processed under appropriate technical and organisational security measures
- not transferred to a country or territory outside the *European Economic Area* unless that country or territory ensures an adequate level of data protection

Monitoring and regulating activity is the responsibility of the Information Commissioner who has powers to identify, record, approve and direct the activities of data users with reference to the Principles and the law. There is also a Data Protection Tribunal to hear appeals against decisions of the Commissioner. A Register of data users is maintained and individuals have the right to give informed consent to processing and to be given access to data – that is, to establish what data is held about them and to see a copy of any material held. There are some exemptions to meeting the full requirements of the legislation, notably: material used for protecting national security, the prevention and detection of crime, and 'minor' domestic data processing. The full text is available on the Web at:
http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

The legislation has worked tolerably well and the Commissioner appears to be reasonably vigilant regarding the use of personal data in the UK in both the public and private sectors. The Commissioner has commented formally on the UK Government's plans for introducing identity cards and described the need for appropriate safeguards.[17] Recent examples of loss of data by government agencies have also come under his scrutiny.

It will be noted that a condition of European Union based legislation is that data may not transferred to a country or territory outside the *European Economic Area* unless that country or territory ensures an adequate level of data protection. For some time there was concern regarding the exchange of data between the United States of America and Europe. The approach to data protection in the USA is somewhat different and lacks congruence with European practice. The situation was ultimately resolved through the operation of a Safe Harbor arrangement which enables organisations in the USA to be appropriately accredited to exchange personal data.[18]

The Individual as Citizen

It was noted earlier that in a modern knowledge-driven society there is a need for a certain degree of disclosure and exchange, if not pooling, of personal information if that society is to conduct its affairs efficiently, economically and effectively. To take

[17] GREAT BRITAIN. Information Commissioner. *Identity Cards Web Page.* (Accessed: April 2008.) http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/identity_cards.aspx
[18] UNITED STATES. Department of Commerce. *Safe Harbor Workbook.* Washington, US DoC, 2005 http://www.export.gov/safeHarbor/sh_workbook.html

one contextual arena as an example, governments operate on this basis in terms of policies, planning and administration, and they have done so for some time. In the UK, for instance, the first modern national official census of population was undertaken in 1801, and the first to record names took place in 1841. Little could be achieved in terms of progress in social welfare, or economic prosperity without a reasonably accurate and detailed picture of national demography.

In recent times what has changed is the sheer volume of information that is assembled and the way in which it can be, and is, processed, distributed and used through the employment of information technology. The UK government's ambitions regarding the application of technology in e-government are well documented.[19] [20] [21] [22] Much has already been accomplished in connecting the citizen with local and national administrations. These developments do, however, raise concerns regarding the balance, and even tension, between an individual's right to privacy and the nation's need to know, as well as the innate security surrounding such information. While it would be fanciful to equate any modern democratic society with the scenario represented in Orwell's 1984, some may have misgivings as the state and its data processing appears to become more powerful. Recent controversies in the UK regarding the proposal to introduce digital identity cards serve as an example. Widely publicised instances of data loss and disclosure by government agencies add to the concern and do not, in everyone, engender confidence in the state's husbandry of information and its respect for privacy.

The relationship between the individual as citizen, and the state as agent, may be viewed in the context of information use in a variety of applications including: economic planning, public health, education, welfare, social cohesion, law enforcement, crime prevention, and, more recently, countermeasures against terrorism. Thus, a plethora of strategic information is needed on population, employment, migration, illness and mortality, skills and learning, social deprivation, together with crime and punishment. Much of this information is useful and useable at a generalised 'macro' level. The citizen's transactions and interactions with the state, on the other hand, necessarily have to be conducted at a more personal level where identity assurance is critical and where personal information must be disclosed. In this context, the security and integrity of data, as well as its fair use, take on a heightened significance. The state may need to be privy to an individual's state of health, ethnic origin, financial circumstances, dependants and even criminal record, as well as perhaps more mundane matters such as address, age and gender. In some circumstance a complex mix of information is used, an example being road pricing and city congestion charging which entails mapping the location of a vehicle (and its owner or driver) in real time and linking to databases of payments and identity.

---

[19] GREAT BRITAIN. Cabinet Office. *Modernising Government.* London, SO, 1999. (Command Paper: Cm 4310) (Chapter 5 - Information Age Government)
[20] GREAT BRITAIN. Cabinet Office. *Transformational Government Enabled by Technology*. London, SO, 2005. (Command Paper: Cm 6683)
[21] Mayo, E. and Steinberg, T. *The Power of Information: An independent review.* London, Cabinet Office, 2007.
[22] GREAT BRITAIN. Cabinet Office.
The Government's Response to: The Power of Information: An independent review. London, SO, 2007. (Command Paper: Cm 7157)

Crime prevention and detection, and especially countering terrorism, rely on a mass of intelligence gathering and surveillance and, where appropriate and authorised, communications interception. There is a concern that assembly of such data may interfere with the legitimate interests of the law-abiding individual. The adage that "… those who have nothing to hide have nothing to fear…" sometimes rings hollow in the light of the risks of inaccuracy, loss or misuse of such data. The Information Commissioner[23] in a submission to Parliament noted the risks:

> The risks that arise as a result of excessive surveillance affect us individually and affect society as a whole. There can be excessive intrusion into people's lives with hidden, unacceptable and detrimental uses. Mistakes can be made and inaccuracies can occur disrupting individuals' everyday lives as increasing reliance is placed on single central collections of personal information …
>
> For individuals the risk is that they will suffer harm because information about them is:
> • inaccurate, insufficient or out of date;
> • excessive or irrelevant;
> • kept for too long;
> • disclosed to those who ought not to have it;
> • used in unacceptable or unexpected ways beyond their control; or
> • not kept securely.
>
> For society the wider harm can include:
> • excessive intrusion into private life which is widely seen as unacceptable;
> • loss of personal autonomy or dignity;
> • arbitrary decision-making about individuals, or their stigmatisation or exclusion;
> • the growth of excessive organisational power;
> • a climate of fear, suspicion or lack of trust.

Some three years earlier, the Information Commissioner was reported in a newspaper as warning that there was a risk of society:

> … sleepwalking into a surveillance society… [24]

Demonstrating one's identity forms a key component of fighting crime as well as indicating one's entitlement to particular services or access to locations. The UK Government's approach, involving as it does identity cards, has not met with universal approval on ground of cost, practicality and privacy. Commenting on the enabling legislation, the Information Commissioner has expressed concern about the way in which measures have developed, including the creation of a National Identity Register.[25]

> The Identity Cards Act 2006 has now passed into law. Our concerns about some of the central features of the Government's proposals were drawn attention to, and echoed by, parliamentarians during the passage of the legislation. We have expressed long standing concerns that the proposals amounted to much more than a simple identity card and more significant concerns centred upon the creation of a National Identity Register.

---

[23] GREAT BRITAIN. Information Commissioner. *Evidence Submitted by the Information Commissioner to the House of Lords Select Committee on the Constitution Inquiry into 'The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State'* Wilmslow, Information Commissioner's Office, 2007

[24] Beware rise of Big Brother state, warns data watchdog. *The Times*. 16 August 2004.

[25] GREAT BRITAIN. Information Commissioner. *Identity Cards Web Page.* (Accessed: April 2008.) http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/identity_cards.aspx

> Although there were some limited but welcomed changes made during the passage of the legislation, we are still concerned about the extent of the information collected and held by Government and how this will be used in practice. This is particularly true of the 'data trail' recorded when a card is checked, for this has the potential to build up a detailed picture of how individuals live their lives.

Concern is sometimes expressed not simply at the nature and extent of what is collected, but on the way it may be aggregated and used. Here, again, there is a genuine tension between safeguarding privacy and exploiting the optimal use of systems and resources funded by taxpayers' money. The perceived dangers in too centralised an approach to data sharing are balanced against achieving a seamless approach to government administration and the avoidance of what is described as 'silo' thinking and working. Another term used is 'seeking joined-up government'. In the United States, the concept of data fusion centres through which data may be aggregated and analysed to counter crime is gaining currency. It is defined in a book of Guidelines[26] published by the Department of Justice as:

> …..an effective and efficient mechanism to exchange information and intelligence, maximise resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources.

Somewhat reassuringly, the Guidelines for managing fusion centres emphasise the need to ensure that constitutional rights, civil liberties, civil rights, and privacy are protected throughout the intelligence process.

The Individual and the Library and Information Service

Managing services focused upon people and information clearly places ethical and legal obligations regarding personal information upon managers in library and information services. Personal information is employed in a variety of applications and tasks in the conduct of their business. Activity may involve interactions with a range of people including: members of funding and governing bodies, equipment and material vendors, employees, supporters and last, but not least, their client base of users and potential users. Typical applications involving personal data include:

- Membership records of users and (possibly) their interests
- Material issue/circulation records
- Records of services provided, and to be provided to users
- Specialist information files on people and organisations, (for example, local community groups, Friends of the Library)
- Staff/personnel files, including payroll files
- Accounts/Invoices and order files
- Electronic mail
- Personal data may also held in databases and catalogues of material, (for example, OPAC's with personal author names) and web pages

Efforts to promote special services, to target particular groups, or to enhance the range and scope of services offered may involve the collection and analysis of more specific

[26] UNITED STATES. Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washintgton, US DoJ, 2006. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

information regarding individuals in the service domain. Community profiling assists in focusing resources on services to groups with special interests and needs. Examples in the public library include: information on visually impaired persons, the elderly and children, or those with an interest in family history. Instances in the academic library may include data on the particular requirements of distance learners or those with dyslexia or visual impairment. In addition, algorithms applied to book loans data enable the assembly and presentation of 'suggested reading' recommendations derived from user borrowing patterns in a similar manner to Amazon's customer-oriented approach. Clearly all these efforts are directed towards improving and targeting services but they do entail the acquisition of additional and, sometimes, sensitive personal information which may be regarded by some as intrusive and trespassing on privacy. A study in the UK reported in 2002, however, indicated that library users were not, in general, greatly anxious about matters affecting their privacy. Moreover, there was a reasonable level of confidence, as well as high expectation, in the way library and information services managed their personal data. It was also revealed that managers would benefit from guidelines on policy and best practice in this area. [27]

A more serious encroachment on privacy relates to the demands and dilemmas that managers may occasionally face when they receive requests from law enforcement authorities to disclose details of individual information use and borrowing habits to assist with the detection of crime or terrorism. Ethical and professional issues relating to confidentiality collide with wider social considerations and legal requirements. In general, managers guard such information jealously to keep faith with their users and they respond only to directives from the courts or judiciary.

In the United States, managers of library and information services, and the public have become particularly concerned about the incidence of visits and enquiries by law enforcement agents, including FBI agents, particularly since the events of September 11, 2001, and the subsequent passage of the Patriot Act,[28] as well as the use of National Security Letters to support investigations. The profession has reacted positively to protect individual privacy through appropriate checks and balances. The American Library Association[29] has provided extensive support and advice in this area.

The seductive attractions of the short term expedient threaten to obscure a deeper principle through which society protects itself, and by which it is judged. Benjamin Franklin put it very succinctly:

> Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.

---

[27] Sturges, P., Davies, J.E., Dearnley, J., Iliffe, U and Oppenheim, C. *Privacy in the Digital Library Environment*. London, Resource, 2002. (Library and Information Commission Research Report 135).
[28] UNITED STATES. Laws, Statutes. *USA Patriot Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.* 2001
[29] AMERICAN LIBRARY ASSOCIATION. *Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff Web Page*. (Accessed: April 2008) http://www.ala.org/ala/oif/ifissues/confidentiality.cfm

Guidance on Professional Ethics

It is appropriate to ponder, how, in the turbulence and uncertainty of everyday management, and faced with sometimes conflicting priorities and demands, does the library and information service manager decide the most ethical path to take? In addition to the requirements of law and one's own conscience, the principles, guidelines and codes of ethics that have become available from a variety of professional organisations now help determine the boundaries of ethical and professional behaviour. They serve as yardsticks by which decisions may be measured and subsequently judged. Throughout the world many such examples exist and the IFLA website offers an extensive list with appropriate links.

The four chosen here for illustration are unequivocal in upholding the importance of privacy as the extracts will demonstrate.

- **The Chartered Institute of Library and Information Professionals [United Kingdom]** [30]

Twelve *Ethical Principles for Library and Information Professionals* that characterise conduct are enumerated. Two are particularly pertinent:

> Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights.
>
> Respect for confidentiality and privacy in dealing with information users.

Additionally, the *Code of Professional Practice for Library and Information Professionals* prescribes professional behaviour in five categories:

A. Personal Responsibilities
B. Responsibilities to Information and its Users
C. Responsibilities to Colleagues and the Information Community
D. Responsibilities to Society
E. Responsibilities as Employees

These are supported by case studies which amplify the interpretation.

Privacy and confidentiality are covered in:

> B. Responsibilities to Information and its Users
>
> 4.Protect the confidentiality of all matters relating to information users, including their enquiries, any services to be provided, and any aspects of the users' personal circumstances or business

and

> D. Responsibilities to Society
>
> 3.Strive to achieve an appropriate balance within the law between demands from information users, the need to respect confidentiality, the terms of their employment, the public good and the responsibilities outlined in this Code.

- **American Library Association [USA]** [31]

[30] CHARTERED INSTITUTE of LIBRARY and INFORMATION PROFESSIONALS. CILIP Professional Ethics Web Page. (Accessed: April 2008) http://www.cilip.org.uk/policyadvocacy/ethics

[31] AMERICAN LIBRARY ASSOCIATION. *ALA Code of Ethics Web Page.* (Accessed: April 2008)

The *ALA Code of Ethics* adopted in 1997 and amended in 2008 comprises eight statements of professional behaviour and includes the following relating to personal information and privacy:

> We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.

In addition, The ALA has been very active in developing policy and advice regarding the Patriot Act, as noted earlier.

- **Australian Library and Information Association** [32]

The *ALIA Statement on professional conduct* specifies the underlying principle governing behaviour together with a general statement about the standards and responsibilities that should be upheld. These are further described in nine separate action statements.

> Principle: People engaged in library and information services are members of a profession committed to intellectual freedom and the free flow of ideas and information.
>
> Statement: Because of the role of library and information services in fostering the social, cultural and economic well being of their communities the people who work in those services have responsibilities for collecting, organising and providing access to information for the clients of their services. The interactions between library and information services and their clients should be guided by the highest standards of service quality and characterised by the highest levels of integrity.

The fourth and ninth statements are relevant to privacy issues.

> protecting their clients' rights to privacy and confidentiality
>
> and
>
> treating clients and colleagues with respect.

- **Canadian Library Association** [33]

The Canadian Library Association *Code of Ethics*, adopted in 1976, is notably brief with its four clauses that succinctly describe the individual and collective responsibility required of membership. The final one addresses privacy issues matters.

---

http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.cfm

[32] AUSTRALIAN LIBRARY and INFORMATION ASSOCIATION. *ALIA Statement on Professional Conduct Web Page.* (Accessed: April 2008)
http://www.alia.org.au/policies/professional.conduct.html

[33] CANADIAN LIBRARY ASSOCIATION.
CLA Position Statements Web Page. (Accessed: April 2008)
http://www.cla.ca/AM/Template.cfm?Section=Position_Statements&Template=/CM/HTMLDisplay.cfm&ContentID=4912

> Members … have the individual and collective responsibility to:
>
> protect the privacy and dignity of library users and staff.

In addition, its Statement on *Citizenship Access to Information Data Banks - Right to Privacy*, also includes the following policy:

> That names of library users not be released to any person, institution, association or agency for any reasons save as may be legally required by Federal or Provincial laws.

Conclusion

Library and information services have a long tradition of providing access to information for all, without hindrance or qualification, and with a regard for the individual's right to freedom and security. It is appropriate for professionals to become involved in discussions regarding the use and protection of personal information throughout the world. This includes respect for individual privacy as well as attention to the reliability and fair use of information about people. Library and information managers, with their background and expertise in gathering, organising and exploiting information, as well as their professional ethos of service and equity are well placed to contribute to the development of policies and practices which ensure that personal information is accorded appropriate treatment, now and in the future.