SUPREMO AMICUS

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

TECHNOLOGY AND PRIVACY ISSUES

By: Malvika Gupta & Radhika Mohan
From: Amity Law School, Noida

ABSTRACT

The aim of this paper is to assess the impact of technology on the private lives of people. It is approached from a socio-ethical perspective with specific emphasis on the implication for the information profession. The issues discussed are the concept privacy, he influence of technology on the processing of personal and private information, the relevance of this influence for the information profession, and proposed solutions to these ethical issues for the information profession.

The three primary thrusts of this paper are: first, that people do not think enough about their own privacy, in particular, they may not know enough about their privacy that they can really make informed decisions about sharing information; second, that technologies exist that can mitigate some of the problems associated with information sharing; and third, that services (in addition to technologies) might be a reasonable way to think about addressing the privacy problem..

1. INTRODUCTION

We are currently living in the so-called information age which can be described as an era were economic activities are mainly information based (an age of informationalization). This is due to the development and use of technology. The main characteristics of this era can be summarized as a rise in the number of knowledge workers, a world that has become more open - in the sense of communication (global village/Gutenberg galaxy) and internationalization (trans-border flow of data).

This paradigm shift brings new ethical and juridical problems which are mainly related to issues such as the right of access to information, the right of privacy which is threatened by the emphasis on the free flow of information, and the protection of the economic interest of the owners of intellectual property.

In this paper the ethical questions related to the right to privacy of the individual which is threatened by the use of technology will be discussed. Specific attention will be given to the challenges these ethical problems pose to the information professional. A number of practical guidelines, based on ethical norms will be laid down.

2. ETHICS

The ethical actions of a person can be described in general terms as those actions which are performed within the criterium of what is regarded as good. It relates thus to the question of what is good or bad in terms of human actions. According to Spinello (1995, p. 14) the purpose of ethics is to help us behave honorably and attain those basic goods that make us more fully human.

3. THE CONCEPT OF PRIVACY

3.1. Definition of Privacy

Privacy can be defined as an individual

condition of life characterized by exclusion from publicity (Neetling et al., 1996, p. 36). The concept follows from the right to be left alone (Stair, 1992, p. 635; Shank, 1986, p. 12)1 . Shank (1986, p. 13) states that such a perception of privacy set the course for passing of privacy laws in the United States for the ninety years that followed. As such privacy could be regarded as a natural right which provides the foundation for the legal right. The right to privacy is therefore protected under private law.

The legal right to privacy is constitutionally protected in most democratic societies. This constitutional right is expressed in a variety of legislative forms. Examples include the Privacy Act (1974) in the USA, the proposed Open Democracy Act in South Africa (1996) and the Data Protection Act in England. During 1994 Australia also accepted a Privacy Charter containing 18 privacy principles which describe the right of a citizen concerning personal privacy as effected by handling of information by the state (Collier, 1994, p. 44-45). The Organization for Economic and Coordination and Development (OECD) also accepted in 1980 the Guidelines for the Protection of Privacy and Transborder Flow of Personal Data (Collier, 1994, p. 41).

Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy. There is thus a relationship between privacy, freedom and human dignity. Respecting a person's privacy is to acknowledge such a person's right to freedom and to recognize that individual as an autonomous human being.

The duty to respect a person's privacy is furthermore a prima facie duty. In other words, it is not an absolute duty that does not allow for exceptions. Two examples can be given. Firstly, the police may violate a criminal's privacy by spying or by seizing personal documents (McGarry, 1993, p. 178)2 . A government also has the right to gather private and personal information from its citizens with the aim of ensuring order and harmony in society (Ware, 1993:205). The right to privacy (as an expression of individual freedom) is thus confined by social responsibility.

3.2. Different Categories of Private Information

Based on the juridical definition of privacy, two important aspects which are of specific relevance for the information profession must be emphasized. The first is the fact that privacy as a concept is closely related to information - in terms of the definition of Neethling (1996, p. 35) privacy refers to the entirety of facts and information which is applicable to a person in a state of isolation. The fact that privacy is expressed by means of information, implies that it is possible to distinguish different categories of privacy namely, private communications, information which relates to the privacy of a person's body, other personal information, and information with regard to a person's possessions. Each of these categories will be briefly dealt with.

Private communications. This category of privacy concerns all forms of personal communication which a person wishes to keep private. The information exchanged during a reference interview between the user and the information professional can be seen as an example.

Privacy of the body (Westin, 1967, p. 351). This normally refers to medical information and enjoys separate legal protection (Neethling, 1991, p. 35-36). According to this legislation a person has the right to be informed about the nature of an illness as well as the implications thereof. Such a person further has the right to privacy about the nature of the illness and can not be forced to make it known to others. The only exception is when the health, and possibly the lives of others may be endangered by the specific illness - such as the case may be where a person is HIV positive and the chance exists that other people may contract the virus.3 This category of information is of specific importance for an information professional working in a medical library.

*Personal information.*Personal information refers to those categories of information which refer to only that specific person, for example bibliographic (name, address) and financial information. This type of information is of relevance to all categories of information professionals.

*Information about one's possessions.*This information is closely related to property right. According to this a person does have control over the information which relates to personal possessions in certain instances. For example, a person may keep private the information aboutthe place where a wallet is kept.

3.3. The Expressed Will to Privacy

The following important aspect of privacy is the desire for privacy (by means of an expressed will) since this desire is important for the delimitation of privacy. In short, the desire for privacy implies that privacy will only be at issue in cases where there is a clear expression of a desire for privacy. For example, a personal conversation between two persons will be regarded as private as long as there is an expressed will to keep it private. The moment that this will is relinquished the information is no longer regarded as private. The same applies to the other categories of personal and private information. If a person makes a private telephone number (as a form of personal information) known to a company, it is no longer regarded as private information. According to the law it can then even be seen as business information which may legally be traded in. This expressed will to privacy acts therefore as a very important guideline for the information professional regarding the delimitation of privacy.

3.4. The Relationship Between Privacy and Confidentiality (Secrecy)

It is also important to distinguish between privacy and confidentiality/secrecy. The confidential treatment of information is not only applicable to the above-mentioned four categories of private and personal information - it may refer to any category of information, such as, inter alia, trade secrets.

4. THE INFLUENCE OF TECHNOLOGY ON THE PROCESSING OF PERSONAL AND PRIVATE INFORMATION

4.1. Definition of Information Technology

Before the influence of the use of technology in the processing of personal and private information can be dealt with, it is important to briefly pay attention to the concept technology. For the purpose of this paper the definition of Van Brakel (1989, p. 240) will be used, namely: the gathering, organizing, storage and distribution of information in various formats by means of computer and telecommunications techniques based on micro-electronics.

4.2. The Ethical Implications for the Use of Technology in the Processing of Information

Although technology has a major impact on the gathering, storage, retrieval and dissemination of information its main ethical impact relates to accessibility/inaccessibility and the manipulation of information. It creates the possibility of wider as well as simultaneous access to information. By implication, it becomes easier to access a person's private information by more people. On the other hand, a person can be excluded from necessary information in electronic format by means of a variety of security measures such as passwords.

The technological manipulation of information refers, among others, to the integration of information (merging of documents), the repackaging thereof (translations and the integration of textual and graphical formats) and the possible altering of information (changing of photographic images) by electronic means.

The use of technology in the processing of information can therefore not be seen as ethically neutral. Christians (199, p. 7) refers to the use of technology as a value laden process. Kluge (1994, p. 337) even comments that technology has changed the ontological status of a document with accompanying ethical implications. By this he specifically refers to the manipulation of information by means of technology.

Brown (1990, p. 3) however on the other hand, indicates correctly that the ethical problems that are caused by the use of technology do not imply - as he puts it - "...that we should rethink our moral values".
The impact of the use of technology on the privacy of people manifests itself in a variety of areas. These areas include, inter alia the following:

The electronic monitoring of people in the workplace. This relates to personal information as discussed earlier. This is done by so-called electronic eyes. The justification by companies for the use of such technology is to increase productivity. Stair (1992, p. 655), however, in the discussion of this practice, clearly points out the ethical problem pertaining to the use of these technologies. According to him peoples' privacy in the workplace are threatened by these devices. It can also lead to a feeling of fear and of all ways being watched - the so-called panopticon phenomenon.

The interception and reading of E-mail messages. This poses an ethical problem which relates to the private communication of an individual. It is technically possible to intercept E-mail messages, and the reading thereof is normally justified by companies because they firstly see the technology infrastructure (E-mail) as a resource belonging to the company and not the individual, and secondly messages are intercepted to check on people to see whether they use the facility for private reasons or to do their job.5

The merging of databases which contains personal information. This is also known as databanking (Frocht& Thomas, 1994, p. 24). By this is meant the integration of personal information from a variety of databases into one central database. The problem here does not in the first place arise from the integration of the information as such. The main problems include the fact that the individual is not aware of personal information being integrated into a central database, that the individual does not know the purpose/s for which the integration is effected, or by whom or for whose benefit the new database is constructed and whether the information is accurate.6 In order to counter these problems relating to privacy and the merging of databases the American Congress passed the Computer Matching and Privacy Protection Act in the 1980s (Benjamin, 1991, p. 11).

Closely related to the merging of files is the increasing use of buying cards ("frequent-shopper cards") by retail stores. Inside such a card a computer chip is buried that records every item purchased along with a variety of personal information of the buyer (Branscomb, 1995, p. 19). This information obtained from the card enables marketing companies to do targeted marketing to specific individuals because the buying habits as well as other personal information of people are known.

Another major threat to privacy is the raise of so called hackers and crackers which break into computer systems (Benjamin, 1991, p. 7). This coincides with the shift in ethical values and the emergence of the cyberpunk culture with the motto of "information wants to be free".

The development of software that makes the decoding of digital information (which can be private information) virtually impossible also poses serious legal as well as ethical questions because it can protect criminals. A good example is the development of software called Pretty Good Privacy by P Zimmerman in 1991. According to an article in the IT Review (1996, p. 22) he has developed the most complex algorithm ever invented which makes the decoding of digital information virtually impossible.

4.3. The Individual and Socio-economical Effect

The use of technology for the processing of personal and other forms of private information has far reaching effects on society. The following effects can be distinguished:

On the individual level: The effect on the individual can be summarized as a loss of dignity and spontaneity, as well as a threat to freedom and the right to privacy. In her research on the impact of technology on the privacy of the individual, Rosenberg (1994, p. 228) concluded that: "Technology continuous to be viewed as a threat to privacy rather than a possible solution". A survey that was conducted in 1990 by Equifax (one of the three biggest credit bureau companies in the USA) on the use of technology and the threat to the privacy of people, found that 79% of the respondents indicated that they were weary of the use of technology for the processing of their personal information (Frocht& Thomas, 1994, p. 24).

On the economic and social levels the biggest effect is the growth of large information businesses like credit bureau and telecommunication companies that specialize in the processing and trade of person-related information. This brings about a redefinition of the role of society (big businesses) in the personal and private lives of the individual (the use of personal information as a commodity). It also becomes clear that the legislation (for example on E-mail) on the protection of the privacy of the individual is falling behind due to the rapidly changing world of technology.

5. THE RELEVANCE FOR THE INFORMATION PROFESSIONAL

The above-mentioned has implications for the information professional on at least three levels. Firstly, the information professional works with all four categories of personal and private information. Secondly, increasing use is made of technology in the processing thereof. Lastly, a new profession is emerging in the infopreneur whose main line of business may be the buying and selling of person-related and other private information.

5.1. The Main Ethical Issues

In the handling and processing of these different categories of private and personal information the information professional is confronted with the following ethical issues:
Deciding which categories of personal and private information the information professional is entitled to gather. This question is of utmost importance to infopreneurs.

The confidential treatment of such information. This issue refers specifically to information gained from the reference interview. According to Froehlich (1994), Smith (1994) and Shaver et al. (1985), the main ethical problems in this regard (with specific reference to online searching) are as follows: can personal details, obtained from the reference interview, be used for purposes other than for that which it was specifically gathered, is it ethically correct to re-use a search strategy formulated for one user for anther user?, is it appropriate to discuss the nature of a specific query with other people?
The accuracy of information. This issue is of specific importance in cases where an information professional is working with personal information that can have a direct influence on the life of a person. An example is the processing of medical information.

The purposes for which various categories of information may be used. The question here is whether an information professional may use any of these four categories of private information for any other reasons than the original reason given for the gathering thereof. Relating to this is the question whether the person must be notified about the way in which personal information is going to be used.

The rights of a person in terms of the use and distribution of one's personal and private information. This ethical problem relates to the above-mentioned questions and boils down to the question of consent of the user in terms of the use of personal information. Related questions are as follows: does a user have the right to verify any personal and private information that is being held by an information professional, and if so, what are such person's rights regarding the correcting (in cases of the incorrectness thereof) of this information, and, does the person have the right to know who is using that personal and private information and for what purposes?

5.2. Applicable Ethical Norms

Applicable ethical norms which can act as guidelines as well as instruments of measurement must be formulated to address these ethical issues. The following norms can be distinguished: truth, freedom and human rights. They will be discussed briefly.

Truth. Truth as an ethical norm has a dual ethical application. Firstly, it serves as norm for the factual correctness of information. As a norm it thus guides the information professional regarding the accurate and factually correct handling of private information. In the second place truth is an expression of ethical virtues such as openness, honesty and trustworthiness.

Freedom. According to this norm a person has the freedom to make choices in terms of freedom of privacy and freedom from intrusion. As norm, however, it may not become absolutized. Therefore the choice to privacy from intrusion may not restrict the freedom of others.

Human rights. This norm is closely related to freedom, but can be regarded as a more concretely applicable norm. Applied to privacy it means the juridical acknowledgment and protection of a persons' right to privacy. As an individual human right it also protects the individual from unlawful interference from society (amongst others the state) in the private life of an individual.

5.3. Ethical Guidelines for the Information Professional

Based on these norms, practical guidelines for the information professional can be formulated. Before the formulation of these guidelines, two fundamental aspects must be taken into consideration, namely the recognition of a persons' autonomy and freedom as well as the fact that the legal guidelines on privacy do not offer a complete framework for the ethical actions of the information professional with regard to the handling of personal and private information.

The concepts of autonomy and freedom has already been dealt with. With regard to the juridical guidelines the following comments can be made. Firstly, once a person's private or personal information has been made known publicly (disclaim of the implied intention) such information is no longer, according to the law, viewed as private. This implies that the information can legally be dealt with as trade information. There is therefore (from a juridical perspective) no ethical sensitivity for the autonomy and freedom of the individual with regard to his right to privacy. The second remark relates to the content of legislation itself. As indicated, the immense growth in and development of information technology give rise to the fact that the legislators fall behind in the tabling of appropriate legislation on the protection of personal privacy. This is especially true in the South African situation where there is, for example no legislation on the protection of privacy to provide for information handled via E-mail.

Bearing in mind these two aspects the following practical guidelines can be given:

(The appropriate norms are also given)
As an acknowledgment of the autonomy and freedom of the individual the information professional must act on the assumption that the client regards as confidential all personal and private information that is handled by the information professional. This implies that the information professional acknowledges the right of the client to control to a certain extent any personal and private information8 - based on the norm of freedom.

The client must, on a regular basis have access to all private and personal information that is held and used by the information professional. The reason for this is to provide the client the opportunity to verify the accuracy of the information. It is then the responsibility of the information professional to see to it that the necessary corrections are made and again verified by the client (Fouty, 1993, p. 290) - based on the norms of freedom and human rights.

The merging of personal and other private information of an individual into a different database than the one for which it was originally collected must be done with the necessary caution (Schattuck, 1995, p. 310). This is specifically applicable in situations where the client is not aware of such merging or the implications thereof. The appropriate action would not only be to inform the client about such a merging and the implications thereof, but also to give the client the right of access to the information on the central database, and the opportunity to change the information where it is incorrect, and the right to know who is using the information as well as the purpose of such use - based on the norms of human rights, freedom and truth.

The information professional must notify the client explicitly of the intended purposes9 of the use of all personal and private information. This implies the client's permission. Different avenues exist for seeking such permission. Spinello (1995:122) prefers the method of implicit informed consent. According to this principle, companies (information professionals) that have collected information about a person must diligently inform that person about the various uses of the information. Clients must then be given an opportunity to consent to these uses or to withhold their consent. The burden is on the client to respond, and a lack of response implies consent. However, the client must be granted the opportunity to withdraw consent (Amidon, 1992:67) - based on the norms of freedom and human rights.

No unnecessary private information must be gathered. This is not only for logistic reasons but also to prevent the unnecessary violation or exposure of a person's privacy - based on the norm of freedom.

Personal and other private information that is no longer necessary for the function for which it was collected must be destroyed (Branscomb, 1995, p. 71) - based on the norms of freedom and human rights.

When the rendering of a specific service or product to a person is refused on the grounds of personal information (e.g. creditworthiness), the reason for this denial must be made known to the person10 - based on the norms of truth and human rights.

A person's information must be handled with the necessary confidentiality. This implies security and control of access to the information, of the right to use it, as well as the right to change or add any information (Fouty, 1993:290) - based on the norms of freedom, truth and human rights.

A private policy must be formulated consisting of the following elements: the categories of information that must be regarded as private and personal, the levels of confidentiality (e.g. who has access and use of which information), a clear explanation of the purposes of the use of the information, and the description of the procedures to ensure the accuracy of this information - based on the norms of freedom, truth and human rights.

6. CONCLUSION

It can thus be concluded that the use of technology in the processing of information poses important questions with regard to a person's right to privacy. This right is directly linked to the right to freedom and human autonomy.

These problems relate mainly to the accessibility of information and the manipulation thereof. This is of specific relevance to the information professional who deals with private and personal information. Practical guidelines in the handling of these problems can be formulated according to the norms of freedom, truth and human rights.

REFERENCES

Amidon, P. (1992). Widening privacy concerns. *Online*, 16 (4): 64-67.

Baker, L. (1992). Needed: An ethical code for library administrators. *Journal of Library Administration*, 16 (4): 1-17.

Benjamin, L.M. (1991). Privacy, computers and personal information: Towards equality and equity in an information age. *Communications and the Law*, 13 (2): 3-16.

Branscomb, A.W. (1994). *Who Owns Information?: From Privacy to Private Access. New York: Basic Books.*A division of Harper Collins Publishers.

Christians, C.G. (1991). Information ethics in a complicated age.In *Ethics and the Librarian. Proceedings of the Allerton Park Institute 29-31 October 1989,* University of Illinois, Graduate School of Library, edited by F.W. Lancaster. Vol. 31. Also In Cochrane, J. (1991).Hell hound on my trail. Ethics and librarianship.*New Zealand Libraries*, 46 (11):2 6-31.

Collier, G. (1994). Information privacy. Just how private are the details of individuals in a company's database? *Information Management and Computer Security*, 3 (1): 41-45.

Focht, K.T. & Thomas, D.S. (1994). Information compilation and disbursement: moral, legal and ethical considerations. *Information Management and Computer Security*, 2 (2): 23-28.

Fouty, K.G. (1993). Online patron records and privacy: Service vs Security. *The Journal of Academic Librarianship*, 19 (5): 289-293.

Froehlich, T.J. (1994). Re-thinking ethical issues in an online environment.*Online Information '94 Proceedings, 6-8 December 1994*, edited by D.I. Raitt& B. Jeapes. Oxford: Learned Information. pp. 415-422.

Goode, J & Johnson, M. (1991). Putting out the flames: The etiquette and law of e-mail.

Online, 15 (6): 61-66.

I spy.Personal rights in the information age. (1996). Information Technology.

Kluge, E.H.W. (1994).Health information, the fair information principles and ethics.*Methods of Information in Medicine,* 33: 336-345.

McGarry, K. (1993). *The Changing Context of Information.An Introductory Analysis.* 2nd ed. London: Library Association Publishing.

Neethling, J. (1991). *Persoonlikheidsreg. Derdeuitgawe*. Durban: Butterworths.

Neethling, J., Potgieter, J.M. &Visser, P.J. 1996. *Neethling's law of personality*.Durban: Butterworths.

Rosenberg, R.S. (1993). Free speech, pornography, sexual harassment, and electronic networks.*The Information Society*, 9: 285-331.

Shank, R. (1986, Summer). Privacy: History, legal, social, and ethical aspects. *Library Trends*, pp. 7-15.

Shattucks, J. (1995). Computer matching is a serious threat to individual rights. In *Computers, Ethics and Social Values*, edited by D.G. Johnson & H. Nissenbaum. New Jersey: Prentice-Hall. pp. 305-311.

Shaver, D.B. et al. (1985, Fall).Ethics for online intermediaries.*Special Libraries*, Fall: 238-245.

Smith, M.M. (1994). Online information ethics: Online searching and the searching self. *Proceedings of the 15th National Online Meeting, May 1994*, edited by M.E. Williams. Medford, NY: Learned Information. pp. 399-405.

Spinello, R.A. (1995). *Ethical Aspects of Information Technology*. New Jersey: Prentice-Hall Inc.

Stair, R.M. (1992).*Principles of Information Systems.A Managerial Approach.*Boston: Boyd & Fraser.

Van Brakel, P.A. (1989). Inligtingstegnologie: Verkenning van navorsingstemas. *Suid-AfrikaanseTydskrifvirBiblioteek- en Inligtingkunde*, 57 (3).

Ware, W.H. (1993). The new faces of privacy. *The Information Society*, 9 (3): 195-211.

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Zorkoczy, P. (1990). *Information Technology: An Introduction*. 2nd edition. London: Pitman Publishing.

*****