# CHAPTER 2
# PRIVACY IN A LEGISLATIVE ENVIRONMENT

## 2.1 INTRODUCTION

Privacy is a basic human need essential for the development and maintenance of both a free society and a mature and stable personality in an individual (Agre & Rotenberg, 1998:193). The right to privacy has become widely recognised and has developed in recent times. It is expressly guaranteed in the Universal Declaration of Human Rights of 1948, the European Convention on Human Rights of 1950, the International Covenant on Civil and Political Rights of 1966, and the American Convention on Human Rights of 1969 (Devenish, 1999:135-136). It is not explicitly mentioned in the African Charter on Human and People's Rights of 1981, but is found in most domestic bills of rights, as is the case in South Africa. The South African Constitution guarantees a number of rights of every South African citizen, including the right to privacy, as described in the Bill of Rights (Constitutional Assembly, 1996).

Since privacy, but more specifically information privacy, is currently on the public agenda in South Africa, with a Committee assigned to improve and add new legislation, this chapter addresses privacy from a legislative perspective to serve as a background for Chapters 3 and 4. It is important for all organisations and associations concerned with managing their customer information process to understand privacy. Any organisation that wants to understand consumers' privacy concerns will have to align its information handling practices and privacy policies with privacy legislation. The purpose of this chapter is to clarify the concept of general privacy before specific privacy issues, such as information privacy, are addressed. The rapid growth and increasing use of information technology (especially the Internet and other electronic means of communication) give rise to many complex privacy and data protection issues. Legislation regulating the data processing industry is essential in view of the threat and potential threat that this industry poses to the personal information of the individual.

This chapter addresses privacy from a constitutional perspective and deals with South Africa's most recent and proposed data protection legislative actions, apart from what is contained in the Constitution. Another important issue discussed in the legislative environment is the increasing perception that adequate privacy protection is a necessary condition for being on the global information highway (Agre & Rotenberg, 1998:112). Since the globalisation of markets has forced governments and international organisations to adopt privacy legislation and actions. Finally, the chapter provides an overview of the history of international legislation since the dawn of the information era has increased the free-flow of personal information across international borders.

## 2.2 THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA

At the beginning of the twentieth century the Cape of Good Hope, Natal, the Orange Free State, and the Transvaal were joined to become the Union of South Africa (Van Wyk, Dugard, De Villiers & Davis, 1996:131). The 1910 Constitution of South Africa gave no rights to the majority of the population and failed to provide for an inclusive democracy. The 1961 Constitution which declared South Africa to be a Republic still denied the majority of the population certain rights. The 1983 Constitution attempted to co-opt the coloured and Indian people as participants in the white-controlled Tri-cameral Parliament, but still excluded black South Africans (African National Congress, 1990:i-iii).

The global political changes of the late 1980s and pressure on South Africa to ban apartheid led to an acknowledgement of the ignored protests of generations of black people in South Africa. The process of developing a constitution for all South Africans started on 2 February 1990, and finally an interim Constitution came into force on 27 April 1994 (Van Wyk *et al.*, 1996:131). Its effect on the South African legal system can justifiably be described as revolutionary. Basically, the interim Constitution brought about three fundamental changes (De Waal, Currie & Erasmus, 2000:2):

- For the first time in South Africa's history, the franchise and associated political and civil rights were accorded to all citizens without racial qualification.
- The doctrine of parliamentary sovereignty was replaced by the doctrine of constitutional supremacy. The Bill of Rights was put in place to safeguard human rights. The courts were empowered to declare invalid any laws and conduct that were inconsistent with the Bill of Rights and the Constitution.
- The strong central government of the past was replaced by a system of government with federal elements. Significant powers were devolved to the provinces and local government.

The 1996 Constitution was drafted and adopted by the Constitutional Assembly and completed South Africa's negotiated political transformation. The Constitutional Assembly was given two years to produce a constitution that conformed to the 34 Constitutional Principles that had been agreed on during the political negotiations from 1991 to 1993. The initial draft of the Constitution was adopted by the Constitutional Assembly on 8 May 1996 and amended on 11 October 1996. Finally, the Constitution was signed into law by President Nelson Mandela at Sharpeville on 4 February 1997 (De Waal *et al.*, 2000:5-6).

The Constitution is an extensive document, numbering 227 pages of print, in the English and Afrikaans versions. Its 251 sections in fifteen chapters, and seven schedules must rank it amongst the longest constitutions in the world (Van Wyk *et al.*, 1996:158). Chapter 2 of the Constitution contains the Bill of Rights. Section 7 in the Constitution declares that the Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in South Africa and affirms the democratic values of human dignity, equality and freedom (Constitutional Assembly, 1996).

## 2.3 THE BILL OF RIGHTS

The 1996 Bill of Rights follows the format of its 1993 Bill of Rights predecessor, and most of the legal changes made in terms of the 1993 Bill of Rights are unaffected by its

replacement by the new Constitution (Jeffery, 1996/97:1). Traditionally, a bill of rights regulates the relationship between an individual and the state. However, the 1996 Bill of Rights goes further than the individual-state relationship – it recognises that private abuse of human rights may be as harmful as a failure to protect individuals from violations against them by the state. For this reason, the Bill of Rights is not confined to the protection of individuals from the state. In certain circumstances, the Bill of Rights also protects individuals against abuses of their rights by other individuals. Section 8(1) in the Constitution describes the circumstances under which the conduct of the **state** may be challenged for being inconsistent with the Bill of Rights. Section 8(2), on the other hand, deals with the circumstances in which the conduct of **private individuals** may be attacked for being inconsistent with the Bill of Rights (De Waal *et al.*, 2000:41). It is clear from Section 8(1) and 8(2) of the Constitution that the Bill of Rights applies both vertically, that is in relation to the state, and horizontally, that is in relation to private persons (Devenish, 1999:24).

Section 7 in the Constitution states that 'the state is obliged to respect, protect, promote and fulfil' the rights in the Bill of Rights (Constitutional Assembly, 1996). This makes the Bill of Rights not just a negative enforcement mechanism shielding subjects against the abuse of government power, but it also imposes a positive duty on the state to protect, promote and fulfil the entrenched rights (Devenish, 1999:8). The Constitution guarantees every South African citizen a number of rights as described in the Bill of Rights. Among these rights are **the right to privacy and the right to access of information**. These two rights are contained in Section 14 (the right to privacy) and Section 32 (the right to access of information) of the Constitution and are discussed below. It is, however, important to mention that Section 36 in the Constitution limits certain rights (including the privacy rights in the Bill of Rights), to the extent that the limitation is reasonable and justifiable in an open and democratic society (Constitutional Assembly, 1996).

## 2.4 THE RIGHT TO PRIVACY

### 2.4.1 Privacy defined

Privacy is a basic human need essential for the development and maintenance both of a free society and of a mature and stable personality in an individual. A logical first step in an evaluation of the law as a mechanism for regulating privacy is to define the scope of privacy law and what is meant by privacy (Agre & Rotenberg, 1998:193). The main problem with regard to privacy is the formulation of a proper definition, since there are different views of this concept. One constant element throughout the history of privacy is the difficulty of defining the concept of privacy. To make matters more problematic, some separate privacy issues such as identity theft and credit card fraud are actually criminal offences unrelated to legitimate uses of information, while telemarketing and unsolicited e-mail marketing are better characterised as sources of annoyance and inconvenience (Loyle, 2002:51). One result of this unsatisfactory situation is the gap between the technical concept of data protection on the one hand, and the legal and moral concept of privacy on the other (Agre & Rotenberg, 1998:6).

The term 'privacy' is widely used to refer to a group of related rights that are accepted nationally and internationally. In an attempt to grasp the scope of the term privacy, some popular privacy definitions are listed below:

- One of the earliest definitions of privacy was documented by Boston attorney Samual Warren and future Supreme Court Justice Louis Brandeis (Warren & Brandeis, 1890:193). They reasoned that the right to life has come to mean the right to enjoy life and that this improved the right to be left alone.
- Konvitz (in McQuoid-Mason, 1978:4) elaborates on the right to be left alone and stated: 'A person may claim the right to be let alone when he acts publicly as when he acts privately. Its essence is the claim that there is a sphere of space that has not been dedicated to the public use or control. It is a kind of space that a man may carry with him into his bedroom or into the street.'

- Fried (in McQuoid-Mason, 1978:5) defines privacy 'not merely as an absence of information about an individual in the minds of others, but rather the individual's control over the information he has about himself'.
- Ruebhausen and Brim (in McQuoid-Mason, 1978:5) argued that the essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself of herself the time and circumstances under which, and most importantly, the extent to which, his or her attitudes, beliefs, behaviour and opinions are to be shared with or withheld from others. They therefore define privacy as 'a positive claim to a status of personal dignity, a claim for freedom of a very special kind'.
- In the Guide to American Law of 1984 (in Devenish, 1999:135), the right to privacy is described as a right based on human dignity and has as its objective the preservation for each individual of 'the choice of when and how much he or she will allow others to know about his or her personal affairs or interfere with his or her mind, or body, or private activities'.
- Longley and Shain (1988:268) provide two definitions of privacy from a data and computer security angle: 'The right of an individual to self-determination as to the degree which an individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations; and the right of individuals and organisations to control the collection, storage and dissemination of their information or information about themselves.'
- In Europe, the right to privacy has been said to consist of 'essentially the right to live one's own life with a minimum of interference. It concerns private family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection from disclosure of information given or received by the individual confidentially' (Devenish, 1999:137).
- The Royal Bank of Canada defines privacy as 'the right of customers to have their personal information safeguarded and to determine for themselves how, and to what

extent, information about them is collected, used and communicated to others' (Jayson, 2002:3).

- In Australia, privacy is defined as 'people's right to the privacy of their own body, private space, privacy of communications, information privacy, and freedom from surveillance' (Collier, 1995:44).
- Privacy is defined in South Africa by Neethling *et al.* (1996:36) as 'an individual condition of life characterised by exclusion from publicity'. This condition includes all those personal facts which the person himself or herself at the relevant time determines should be excluded from the knowledge of outsiders and in respect of which (s)he evidences a will for privacy.

Westin (in Agre & Rotenberg, 1998:194) contends that no final and absolute definition of privacy is possible because privacy issues are fundamentally matters of values, interests, and power. Privacy itself is an intangible commodity and is often mentioned in a negative context. For example, privacy is 'invaded', a confidence is 'breached', or a trust is 'broken' (Pounder & Kosten, 1992:1). Violations of privacy can constitute an invasion of a person's private life or relate to the acquisition and disclosure of personal information. The invasion of privacy has been defined as 'an international and wrongful interference with another's right to seclusion in his or her private life' (Devenish, 1999:145). Because of invasions of privacy, the Constitution addresses the right to privacy in Section 14 of the Bill of Rights.

For the purposes of this study, two definitions were developed (based on the above discussion) to define **privacy** and **information privacy** as they relate to the issues addressed in Chapters 2, 3 and 4.

**Privacy** is defined **as the right of an individual to isolate his or her private life (personal facts, time, circumstances, values and interests) from the knowledge of others, to be able to control what is withheld from others, and to be free from wrongful interference in his or her private life.**

**Information privacy** is defined **as the right of an individual to safeguard information about himself or herself from the use or control by others.**

### 2.4.2 Section 14 on the right to privacy

Section 14 in the Bill of Rights of the Constitution of the Republic of South Africa, which embodies the right to privacy, states (Constitutional Assembly, 1996):

> Everyone has the right to privacy, which includes the right not to have:
> - Their person or home searched;
> - Their property searched;
> - Their possessions seized; or
> - The privacy of their communications infringed.

Section 14 in the Bill of Rights has two parts. The first guarantees a general right to privacy (discussed in Section 2.4.2.1 of this study), and the second protects people against specific infringements of privacy, namely searches and seizures, and infringements of the privacy of communications (discussed in Section 2.4.2.2 of this study). Usually, the two parts are dealt with in separate sections of a bill of rights. In South Africa, however, the specific areas of protection form part of the general right to privacy. In most cases, when one's person, home or property is searched, or when one's possessions are seized or communications intercepted, Section 14 would be infringed upon. However, because the right against searches and seizures is a subordinate element of the right to privacy, the Constitution's protection is triggered only when an applicant shows that a search, seizure or interception of communication has infringed the general right to privacy (De Waal *et al.*, 2000:242-3).

#### *2.4.2.1 The general right to privacy*

An individual's general right to privacy is protected by common law as well as by the Constitution. Common law recognises the right to privacy as an independent personality

right and the Constitution recognises the right to privacy as a human right. This section of the study provides a brief description of the general right to privacy as protected by South African law.

*(a) The common law right to privacy*

The same considerations that have led to the entrenchment of a right to privacy in the Bill of Rights have long been recognised by common law as important reasons for protecting privacy. Common law recognises the right to privacy as an independent personality right which the courts consider to be part of the concept of a person's 'dignitas'. In common law, the breach of a person's privacy constitutes an *iniuria*. This occurs when there is an unlawful intrusion on someone's personal privacy or an unlawful disclosure of private facts about a person. Some examples of breaches of privacy recognised by the common law include entering a private residence; reading private documents; listening in on private conversations; shadowing a person; disclosing private facts which have been acquired by a wrongful act of intrusion; and disclosing private facts in breach of the relationship of confidentiality. The courts have also held that the common law right to privacy is invaded by publishing a person's photograph as part of an advertisement without the consent of that person, by a doctor's informing third parties that his or her patient had HIV (human immune deficiency virus), by wire-tapping private premises, and by peeping at a woman while she is undressing (De Waal *et al.*, 2000:243).

Because the South African legal system has entered the human rights arena, the relationship between fundamental human rights and personality rights must be considered briefly. The Bill of Rights recognises certain personality interests such as privacy. Many human rights relate to interests of personality. Personality rights which are enshrined in a bill of rights generally remain subjective rights, but receive stronger protection because the legislature and the executive of the state may not pass any law or take any action which infringes upon or unreasonably limits such rights. Thus, in addition to the normal delictual remedies available in the case of the infringement of a

personality right, these rights receive constitutional guarantees and protection (Neethling *et al.*, 1996:19).

*(b) The constitutional right to privacy*

The Constitutional Court has cautioned against a straightforward use of common law principles to interpret fundamental rights and their limitations. The determination of whether an invasion of the common law right to privacy has taken place is a single enquiry, and involves an assessment as to whether the invasion is unlawful. Under the Constitution, by contrast, a two-stage analysis must be employed in deciding whether there is a violation of the right to privacy. First, the scope of the right must be assessed to determine whether law or conduct has infringed upon the right. Second, if there has been an infringement, it must be determined whether it is justifiable under the limitation clause (De Waal *et al.*, 2000:243-4).

Although privacy is a right, some limitations with regard to it may be essential for the administration of justice and the reasonable maintenance of law and order. The courts should endeavour to find a balance between the public's right to know and the individual's right to privacy (Devenish, 1999:157). The scope of a person's privacy right extends only to aspects of his or her life or conduct where a legitimate expectation of privacy can be harboured. A legitimate expectation means that one must have a 'subjective expectation' of privacy that society recognises as 'objectively reasonable'. The subjective expectation component simply recognises that a person cannot complain about an infringement of privacy if (s)he has consented explicitly or implicitly to having his or her privacy invaded. At the same time, it is rather difficult to assess the kinds of privacy expectations that society would regard as objectively reasonable (De Waal *et al.*, 2000:244).

In modern society, the right to privacy seeks to protect three related concerns. An individual's subjective expectation of privacy in respect of these three concerns is usually regarded by society as objectively reasonable (De Waal *et al.*, 2000:244).

- First, the right to privacy seeks to protect certain aspects of one's life in respect of which one is entitled to be left alone: one's body, certain places and certain relationships. The rationale behind this right is that the state and other people should have nothing to do with an individual's intimate affairs.
- Second, the right to privacy aims to protect the opportunities for an individual to develop his or her personality and therefore extends to certain forms of individual and personal self-realisation or self-fulfilment. The implication is that the state may not compel individuals to conform to a stereotypical view of what a model citizen is. This right to privacy dictates that the state and society should be tolerant towards non-conformists. In this regard, the right to privacy involves issues such as the right to choose the kind of lifestyle one wants to lead.
- Third, the right to privacy seeks to protect the ability of individuals to control the use of private information about themselves. This right is closely related to the right to dignity, since the publication of embarrassing information, or information that places a person in a false light, is often damaging to the dignity of the person. But the right to privacy guarantees control over all private information and it is immaterial whether the information is potentially damaging to a person's dignity or not. The use of a person's name or identity without his or her consent would, for instance, constitute a violation of the right to privacy.

#### *2.4.2.2 Infringements of privacy*

In the field of the protection of privacy, the convictions of the community regarding right and wrong are of particular importance as a criterion of wrongfulness in all countries. This view is also apparent in South African case law. Privacy can be infringed upon only by knowledge of personal facts by outsiders contrary to the determination and will of the person whose right is infringed upon (Neethling *et al.*, 1996:243). The second part of Section 14 of the Bill of Rights protects individuals against specific infringements of privacy, namely searches and seizures, and infringements of the privacy of communications.

*(a) Searches and seizures*

The right to privacy includes the right not to have one's person, home or property searched or one's possessions seized. A violation of privacy by means of an act of intrusion takes place where an outsider acquires knowledge of private and personal facts relating to an individual, contrary to that individual's determination and wishes (Neethling *et al.*, 1996:243). Searches and seizures that invade privacy must be conducted in terms of legislation clearly defining the power to search and seize. There are laws that authorise searches and seizures, the most important of which is the Criminal Procedure Act 51 of 1977. The implication of the right to privacy is that the state or private individuals cannot search private property, the person or the home of others, or seize their possessions unless authorised to do so by statute or by the common law. When a search or a seizure is authorised by law, it is lawful, but the constitutionality of the enabling statute or common law may be attacked for violating the right to privacy (De Waal *et al.*, 2000:256).

*(b) Privacy of communications*

According to South African law, the infringement of private communications constitutes an invasion of privacy. The invasion can be committed by electronic means or by eavesdropping (Devenish, 1999:153). The infringement of privacy through an act of disclosure arises where, contrary to the determination and will of the individual, an outsider reveals to third parties personal facts regarding that individual, which, although known to the outsider, nonetheless remain private. For the sake of convenience, three types of disclosure of private facts can be distinguished, namely, first private facts acquired by a wrongful act of intrusion; second, disclosure of private facts contrary to a confidential relationship; and third, the disclosure of private facts through mass publication.

(i) Wrongful act of intrusion:

If a person acquires knowledge of private facts through a wrongful act of intrusion, any disclosure of those facts by such a person, or by any other person, in principle constitutes an infringement of the right to privacy (Neethling *et al.*, 1996:244). The

embodiment of private facts, for example by photography, photocopying and tape recording, contrary to the determination and will of the individual, constitutes a threat to the right to privacy. Although these acts in themselves do not violate the right to privacy because a wrongful act of intrusion or disclosure of private facts is not present, this interest is exposed to the danger or risk of a wrongful act of intrusion or exposure (Neethling *et al.*, 1996:260).

(ii) Confidential relationships:

Where only selected persons acquire knowledge of private facts in accordance with the determination and will of the plaintiff, and these persons disclose the information, contrary to this determination and will of the person, to a single person (or a small group of persons, as opposed to the mass publication thereof), the wrongfulness of their conduct is more problematic. It is submitted that as a rule, the disclosure is not contrary to the convictions of the community. Giesker (in Neethling *et al.*, 1996:243) suggests that 'the more necessary it is for a person to impart the private facts of the outsider, the more pressing the protection against the disclosure of those facts to third parties by the outsider'. In certain instances the relationship is such that persons are compelled to disclose certain facts about themselves to other parties, such as relationships between doctor and patient, banker and client, direct marketer and consumer. A confidential relationship may also arise where there is an agreement between the parties that private facts disclosed will be confidential or secret (*Geheimhaltungsvertrag*). In such instances disclosure of the private facts involved apart from the breach of contract also constitute an infringement of the right of privacy (Neethling *et al.*, 1996:249-54).

(iii) Mass publication:

The mass publication of facts (disclosure to an unlimited or limited number of persons) is characterised by an element of confidentiality, and the publication thereof in principle infringes on the right to privacy (Neethling *et al.*, 1996:254). The question that must be asked here is to what extent the newspapers may publish truthful – albeit painfully intrusive information – about a person. Newspapers are entitled to publish certain truthful information, although private in nature, about public figures. This is because 'the

candidate who vaunts his spotless record and sterling integrity cannot convincingly cry "foul" when an opponent or an industrious reporter attempts to demonstrate the contrary' (Devenish, 1999:155). Private persons are in an entirely different position, and should enjoy far greater protection. However, it could be argued that the newsworthiness of a particular subject could in practice diminish the extent of such protection. Here the courts have to endeavour to find a balance between the public's right to know and the individual's right to privacy (Devenish, 1999:154).

It is important to note that in all the above-mentioned instances, the question of an infringement of privacy arises only if the individual is identified with the disclosed facts. If this element of identification is absent, the disclosure does not relate to a specific person in his or her state of privacy.

Apart from giving the right to personal privacy a benevolent interpretation, Section 14 must also be read together with similar rights protected in other sections in Chapter 2 of the Bill of Rights, such as the right of access to information provided for in Section 32. The right to personal privacy (Section 14), read with the right of access to information (Section 32), should therefore be interpreted as guaranteeing each citizen a privacy of personal information. The section below addresses the right of access to information as contained in Section 32 of the Constitution.

## 2.5 THE RIGHT OF ACCESS TO INFORMATION

The objective of the Constitution and the Bill of Rights is to create an open and democratic society. By providing a right to freedom of information, the Constitution has recognised the importance of access to official information in the modern era. Freedom of information is based on two levels: first, at an individual level, where freedom of information is closely connected to freedom of expression and the right to privacy; and second, at a level where freedom of information operates at a political level. In an open and democratic society, government should be accountable for its actions and decisions. Public access to information is fundamental to encouraging transparency and

accountability in the way government and public authorities operate. In addition, the Constitution provides a right of access to information in private hands, where that information relates to the exercise or protection of the rights of the information seeker. This provision recognises that information in private hands, such as those of employers, credit bureaux, insurance companies, banks and direct marketers, can have a considerable impact on an individual who should be able to have access to that information in order to ensure its accuracy or to challenge decisions made on the basis of the information (De Waal *et al.*, 2000:41-2).

### 2.5.1 Section 32 on the right of access to information

Section 32 of the Constitution states (Constitutional Assembly, 1996):

> Section 32(1): Everyone has the right of access to:
> (a) Any information held by the state; and
> (b) Any information that is held by another person and that is required for the exercise or protection of any rights.
>
> Section 32(2): National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

Section 32(1) sets out the right of access to information in the hands of the state, but also expands the reach of the right of access to information held by private persons. The second part of Section 32(1), stating the access to information held by 'another person', reflects the horizontal nature of the Constitution. This means that it applies not only vertically between citizens and the state, but also between people, among themselves (Brand, 2000b:3). Regarding the access to information held by the state [Section 32(1)(a)], there are no restrictions, thus providing for a rather wider right. Section 32(1)(b) contains the term 'required', and the right has to be interpreted in such a way that one may exercise the right when the information is reasonably required for

the protection of one's rights. The term 'rights' is not defined in the above context and could be taken to refer to the fundamental rights of a person, private law rights or both legislative and private law rights for which the state is responsible, as well as a private individual. This does not, however, provide for a blanket right to accessing information (Judin & Kisch, 2001:1-2). The Constitution is quite clear about the kind of information that may be requested. In the case of the state, there is access to 'any information'. In the case of private bodies, that access is restricted to information that may be needed to exercise or protect other rights (Brand, 2000d:6). It may be possible to refuse such a request on the basis that it would result in an invasion of the privacy of an identifiable person other than the person requesting the information. Further grounds for refusal may be that the records sought to be attained disclose confidential information about a third party, for example, trade secrets (Judin & Kisch, 2001:1-2).

Important limitations are placed on the type and quantity of information that may be claimed under the rights by the proviso that such information must be made available to an applicant only 'in so far as such information is required for the exercise or protection of any of his or her rights' (De Waal *et al.*, 2000:442). Justifiable limitations can arise in relation to law enforcement and criminal procedure, state secrets and foreign affairs, national security, privacy, trade secrets or confidential business information, and legal professional privilege (Devenish, 1999:447-8). The right of access to information therefore includes a number of exemptions. First, the right applies only to 'records' – that is information recorded either in written or electronic form. This excludes information documents of the cabinet, courts and members of parliament or provincial legislatures. Requests for information may also be refused if they would constitute an unreasonable invasion of third-party privacy. Several further exemptions relate to security, military and economic matters, law enforcement and foreign relations. In the case of privately held information, further exemptions are made to protect commercial interests and trade secrets (Brand, 2000d:6). The right of access to information is thus a balancing process to be used between the right to access and other fundamental rights, such as one's right to privacy (Judin & Kisch, 2001:2).

The **right of access to information** (Section 32) could be beneficial in relation to a judicial review of administrative actions, which provides for the **right to just administrative action** (Section 33). Therefore, where the policies and criteria used by administrative bodies are inaccessible to the public, Section 32 could be invoked to secure the required information, subject to the restrictions sanctioned by the limitation clause (Devenish, 1999:451). The Promotion of Administrative Justice Act 3 of 2000 was instituted to give effect to one's right to administrative action that is lawful, reasonable and procedurally fair, and to the right to written reasons for administrative action as contemplated in Section 33 of the Constitution (Hoexter, Lyster & Currie, 2002:13). The Promotion of Administrative Justice Act 3 of 2000 applies to both the state and to persons other than the state (Lambrechts, 2000:90).

Item 23 of Schedule 6 in the 1996 Constitution suspended the operation of the access to information rights until freedom of information legislation was enacted, or for a maximum period of three years (to the end of January 2000). This means that the right in Section 32(1) could not take effect until the enactment of the required national legislation required by Section 32(2) of the 1996 Constitution. Legislation to give effect to the rights enshrined in Section 32 was addressed via the drafting of the Open Democracy Bill that was promulgated as the Promotion of Access to Information Act (De Waal *et al.*, 2000:42). A description of the development process of the Open Democracy Bill is given below.

### 2.5.2 Promotion of Access to Information Act 2 of 2000

There is a significant difference between the USA and Europe in their approach to privacy. Legislation in the USA is mainly based upon its Bill of Rights, which primarily serves to protect the individual from the state. Legislation to protect the individual from undue invasion of privacy by other legal persons is minimal and fragmented. Legislation in Europe, on the other hand, is more concerned about the protection of the individual from other individuals. In South Africa, the first draft of the Open Democracy Bill conformed more closely to the United States pattern (Department of Communications,

2000b:70). The Open Democracy Bill, which dealt with the constitutionally-guaranteed right of access to information, was introduced in Parliament in 1998 (Brand, 2000a:3). This Bill, ostensibly proposed as a means to entrench these rights particularly in the governmental sector, was extended to include a chapter relating specifically to the rights of privacy and information access in the private sector. The memorandum on the objects of the draft Open Democracy Bill stated, among other things, that the principal objects of the Bill are to provide for 'access by individuals to information about themselves held by private persons, the correction of personal information held by the state or private persons, and the protection of individuals against abuse of their personal information by the state or other private persons' (Direct Marketing Association, 2001a:8).

The above Bill placed stringent and onerous privacy requirements on private organisations. Several industry bodies lobbied for amendments to the Bill. They argued that the initial legislative proposals were inappropriate and that the conditions and limitations would be detrimental to the industry. The Open Democracy Bill was subsequently withdrawn and reintroduced towards the end of 1999. After the private sector portions and data protection provisions of the Open Democracy Bill had been removed, the Bill was approved with 254 votes to 82, and promulgated as the Promotion of Access to Information Act 2 of 2000 (Brand, 2000c:3; Ludski, 2000:1; Direct Marketing Association, 2001a:8). The objective of Act 2 of 2000 is to give effect to the constitutional right contained in Section 32 of the Constitution of access to any information held by the state, as well as any information that is held by another person and that is required for the exercise or protection of any rights (Lambrecths, 2000:86).

In terms of the Promotion of Access to Information Act, all organisations have to produce manuals of information held by the organisation. The South African Human Rights Commission has published a 'blueprint' of what a manual could look like and the information it should contain. The Minister for the Department of Justice has, after several requests, approved an extension to the deadline for the publication of manuals from 15 August 2002 to 28 February 2003 (Ivans & Duval, 2002). The current Promotion

of Access to Information Act thus emphasises the obligations of the state in the protection of personal data held by it more than the collection, use and dissemination of personal data by the private sector.

However, the exclusion of the private sector portions of the Open Democracy Bill was accompanied by a strong plea by the Chair of the Parliamentary Portfolio Committee (Advocate De Lange) to the Law Commission to pass a Data Privacy Law with urgency (Direct Marketing Association, 2001a:8). The constitutional recognition and protection of the right to privacy (Section 14) as a fundamental human right provides some indication of the importance of this right and may possibly place a duty on the state to adopt proper legislation for the regulation of the data industry and the protection of an individual's personal data. Moreover, Section 32 in the Constitution gives individuals access to information held by the state, but also access to any information held by another person (Neethling *et al.*, 1996:292). This highlights the fact that it is important to regulate the data industry. Therefore, the next section of this chapter addresses data protection as related to privacy and freedom of information. Data protection is a descriptive term referring to rules about the collection, use and dissemination of personal information. One important policy objective of data protection is the application of fair information practices, an organised set of values and standards regarding personal information and defining the rights of record subjects and the responsibilities of record keepers (Agre & Rotenberg, 1998:194).

## 2.6 PRIVACY AND DATA PROTECTION

Data protection entails the legal protection of persons (the data subjects) with regard to the processing of data concerning themselves by other persons or institutions (the data media). Since the seventies, the individual's need for protection in this field, which especially concerns his or her privacy as a personality object, has progressively received more attention in industrialised countries (Neethling *et al.*, 1996:291). The processing of private and public data can pose a potential threat to an individual and is briefly discussed below.

### 2.6.1 Private and public data

Private data about an individual can be held by credit bureaux, banks, employers, insurance companies, the medical profession, voluntary associations and mailing list companies. These data media often collect personal information about individuals with regard to various activities such as drinking habits, health, reputation, political and religious convictions, criminal records, race and creditworthiness. Although the data stored by these institutions are often available only to its clients, the possibility exists that other individuals, private institutions or even the state may have access to such information (Neethling *et al.*, 1996:292-4). Mr Johnny de Lange, chairman of the Parliament's justice portfolio committee, claims that the absence of relevant legislation has exposed South Africans to widespread abuses of privacy (Ludski, 2000:1). When people apply for an account at a bank, the personal information obtained by the bank can be shared with other institutions without the consent of customers. Unless it is properly regulated, information technology is capable of eroding, if not eliminating, the concept of privacy. People around the world are increasingly recognising that they and their personal information are subjected to unfair control and manipulation on a daily basis. Therefore, countries around the world are passing legislation on personal data protection (Holvast *et al.*, 2001:14). Data protection is no longer seen as a purely functional construct to be used to directly shape and influence the use of information-processing technology. Instead, the focus has shifted to the individual, as can be seen in citizen's rights featured prominently in all European data-protection systems (Agre & Rotenberg, 1998:235).

The state, with all its departments, agencies and other offices, personifies the public data media. On account of the state's numerous activities and functions, the personal data processed covers a wide range, for example information on civil servants as employees, on pupils and students at educational institutions, on taxpayers at the receiver of revenue, and on all individuals in terms of census reports, voters' rolls and registration of the population. The processing of this data is usually justified by its public

importance. The storage and use of the information is generally essential for the proper functioning of state administration and effective state planning. Since individuals may be compelled by legislation to furnish information on themselves to the state, the state controls this unique source of information directly. To illustrate the danger that the processing of data by the state poses to the privacy of the individual, the Identification Act 72 or 1986 is discussed below. This statute permits the Director-General of Internal Affairs to supply personal information without the consent of the data subject to any other state department, local authority or statutory body for any of their purposes, or even to any other person who makes application and pays the prescribed fees, if the Director-General is of the opinion that furnishing such information is in the interests of the person concerned or in the public interest (Neethling *et al.*, 1996:294-5).

The processing of information by private or public data media threatens individuals in two ways. First, the compilation and distribution of personal information creates a direct threat to the individual's privacy. When information relating to a person is collected, the total picture represented by the record of such facts is usually of such a nature that the person in question would like to restrict others from having knowledge thereof, despite the fact that some of the data, viewed in isolation, are not necessarily 'private'. Second, the acquisition and disclosure of false or misleading data may lead to an infringement of the individual's right to his or her identity. A processing of incorrect or misleading personal data through the data media also poses a threat to an individual's identity because the information is used in a manner which is not in accordance with his or her true personal image (Neethling *et al.*, 1996:295-6).

Unless data legislation controls the private sector in South Africa, the public is justified in being concerned about its personal data privacy. Hence, given the limitations of the Promotion to Access of Information Act, the Law Commission instituted a Project Committee consisting of various experts to investigate the privacy and data protection issue.

### 2.6.2 Project 124 Committee

The Ad Hoc Joint Committee on the Open Democracy Bill submitted its report on the Promotion of Access to Information Bill to Parliament on 24 January 2000. The Committee noted that the Bill only deals with the aspect of access to private information about an individual, be it access by that individual or another person, and did not regulate other aspects of the right to privacy, such as the correction of and control over personal information. Foreign jurisdictions with freedom of information regimes have enacted separate legislation which, as an important component of democracy legislation, regulates aspects such as the correction of and control over personal information. Privacy legislation generally provides for more detailed mechanisms and provisions dealing with personal information in the hands of another person by empowering that individual, among others, to demand the rectification of incorrect information.

The Committee requested the Minister for Justice and Constitutional Development to introduce privacy and data protection legislation in Parliament as soon as possible. Since the preparation of this type of legislation will require extensive research, the Minister requested the Law Commission to consider the possible inclusion of such an investigation in its programme. The Minister then approved the inclusion of the investigation in the Commission's programme on 8 December 2000. At the start of 2002, the Minister of Justice assigned ten members to the Project 124 Committee under the chairmanship of Judge Craig Howie, with Prof. Neethling as the project leader. The Project 124 Committee is currently investigating the privacy and data protection issue with the aim of improving existing legislations and adding new legislation as soon as possible (Mokgoro, 2000:10-22).

**Consumers' expectations and concerns regarding possible legislation and government protection are of specific importance to this study and will be one of the aspects measured in the empirical survey.**

Due to the multifaceted nature of the data industry, it may be necessary for the Project 124 Committee to develop codes of conduct, enforced by legal sanctions, for the data activities for each sector of the data industry. However, this method is likely to be cumbersome and too extensive, and may also prove to be too rigid. Consequently, a more flexible approach seems to be required by means of which general principles may be developed for the protection of data. According to traditional principles, it can be accepted that the unauthorised collection or storage of personal information, or the processing of false or misleading data are in principle wrongful and that the communication thereof to third parties should also be regarded as unlawful (Neethling *et al.*, 1996:297-9). Traditional principles of protection are of little value if a data subject is not legally empowered to exercise direct control over his or her data records.

It is obvious that legislation regulating the data processing industry is essential in view of existing threats and potential threats to the personal information of the individual. Neethling *et al.* (1996:306) stressed the fact that when drafting legislation, a proper balance must be found between competing interests. First, the individual's personality merits proper protection. Second, the Constitution recognises every person's right to engage freely in economic activity. In order to exercise this right properly, an individual needs personal information about others. Third, the state can fulfil its functions properly only if it also keeps a record of sufficient personal information regarding its subjects. Future legislation will have to accommodate all these rights and interests in a balanced manner.

The complexities of modern society have produced more reasons why the state or an individual has an interest in, and need of information regarding another person. In order to obtain this data and satisfy these needs, a new industry has developed, the practices of which pose a potential threat to the individual due to the use of electronic means (computers) for storing data (known as a data bank). In particular, integrated data banks create a greater possibility of disclosure of an individual's private life (including computer privacy) than ever before (Neethling *et al.*, 1996:291). Various role players in South Africa are also aware of the effect of the electronic commerce environment on

information privacy. The section below addresses some of the current issues on the matter.

### 2.6.3 Electronic communications and transactions

Rapid growth in Internet usage has fuelled the privacy issue. In every electronic communication, an Internet user discloses some form of personal information. Every e-mail message contains a header with information about the sender and the recipient. Virtually every electronic transaction involves the transfer of personal data such as identity numbers, credit card numbers, telephone numbers, physical addresses and e-mail addresses. The key to further Internet growth, especially as far as electronic commerce is concerned, is the attainment of privacy through technology and law (Buys, 2002). Buys (2002) contends that it would be risky to regulate the technology that threatens privacy. He believes that the legislature and the courts should rather be interested in giving Internet users control over their own information and to provide measures to enable every user to make an informed decision on the question of how private and confidential personal information should be in the digital age.

In May 1998, the Department of Communications received a mandate to establish an information technology investment cluster. The main objective of this cluster was to develop coherent legislation on information society-related issues (Groenewald & Lehlokoe, 1999). The right to privacy and data protection was a key issue taken up by the Department of Communication in the e-Commerce Green Paper. The Minister of Communications, Dr Ivy Matsepe-Casaburri, launched the government's Green Paper on e-Commerce on 20 November 2000. The launch concluded the first phase of government's initiative to develop an appropriate legal foundation for electronic business in South Africa. The Green Paper invites comments which, when considered and compiled, will direct the formulation of government policy in a White Paper (Department of Communications, 2000a). In the electronic commerce (also called e-commerce or e-business for short) environment, unsolicited commercial e-mail, international sharing of data, automatic collection of information, and tracking of

individuals when they go online are contentious issues. Legislation aimed at preventing any abuse of information and an invasion of privacy is expected to give individuals the right to demand the correction of information that is on record about themselves. It is also expected to stop organisations from using information provided by customers for purposes other than those for which it was supplied (Ludski, 2000:1).

The Electronic Communications and Transactions (ECT) Bill was tabled before Parliament recently and South Africa became the first country in Africa to join more than 20 other countries that have introduced electronic commerce legislation in the past four years (Temkin, 2002:2). The Bill reads *inter alia* as follows:

- to provide for the facilitation and regulation of electronic communications and transactions;
- to provide for the development of a national e-strategy for the Republic;
- to promote universal access to electronic communications and transactions and the use of electronic transactions by small, micro and medium sized enterprises;
- to provide for human resource development in electronic transactions;
- to prevent abuse of information systems;
- to encourage the use of e-Government services; and
- to provide for matters connected therewith (Minister of Communications, 2002).

The Bill will affect all organisations, even if they do not consider themselves e-commerce players. This is because it also deals with issues that go beyond electronic transactions such as the registration of cryptography providers, proper control of critical databases, consumer protection, domain name administration and cyber crime (Temkin, 2002:2). The act aims to give legal effect to and regulate a wide range of electronic communications. These include electronically stored records, e-mail, websites, short message services (SMS), pre-recorded telephone messages, automated teller machine (ATM) transactions and online contracting (Grealy, 2002:21). Any organisation that encrypts documents or messages will be affected by clauses allowing government to determine which technologies can be used and when messages can be intercepted. A proposal that gives government the right to know what kind of critical information is

stored on corporate databases will also affect organisations. Traders selling goods or services online face onerous new rules. Retailers who do not give full details about their company and give consumers sufficient opportunity to review and modify an order would be obliged to take the goods back if the buyers changed their minds within 14 days (Stones, 2002:3; Temkin, 2002:2).

Using a smart card, a fingerprint and a password, President Thabo Mbeki signed into law the Electronic Communications and Transactions (ECT) Bill in July 2002. The ECT Act makes this advanced electronic signature legal. At the signing ceremony, Communications Minister Ivy Matsepe-Casaburri said the Act allowed for data messages to be legally recognised. It would ease the conclusion of deals and transactions online. The most controversial part of the Act is Chapter 10, which allows for a non-profit organisation to control the '.za domain'. This organisation's nine directors will be nominated by the Minister, following a process of public nomination and selection by an independent panel (Anon, 2002c:2).

Because of the ubiquity, ease of use, speed and decentralisation of electronic technology, privacy is unequivocally an international issue on the international agenda. South Africa's policy-makers will have to pay attention to agreements reached at the international level with regard to privacy and data protection (Agre & Rotenberg, 1998:112). Therefore, the final section of Chapter 2 provides a broad outline of the development of international privacy issues, highlighting some of the most important privacy legislation in other countries which might have a bearing on the South African scenario.

## 2.7 INTERNATIONAL PRIVACY AND DATA PROTECTION

The dawn of the information age has increased the importance of personal data protection to a level where governments and international organisations around the world have been forced to adopt privacy legislation and multilateral instruments. At the same time, various organisations and governmental interests have attempted to stem

the tide of public demands for the privacy of an individual's most sensitive private information (Holvast *et al.*, 2001:1). A discussion on the historical development of privacy and data protection in the international arena follows.

### 2.7.1 Before 1970

The first privacy law was created by Warren and Brandeis in the USA in 1890, although it was not until 1970 that the Privacy Act was enacted (Schwartz, 1998:48). On 10 December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. The Declaration sets forth a comprehensive list of the rights to which all people are entitled. Article 12 of the Universal Declaration recognises the right to privacy (Rotenberg, 2001:256). Shortly after the Universal Declaration of Human Rights of the United Nations, the Council of Europe Convention for the Protection of Human Rights was adopted, in 1950. Article 8 in the Council of Europe Convention addresses the right to respect private and family life (Rotenberg, 2001:262). Many believe that the Nazis behaviour was the impetus for the 1950 European Convention on Human Rights, drawn up shortly after World War II. Europeans viewed privacy as a human right partly as a reaction to the Nazis use of personal records to identify 'undesirables' (Williams, 1999:5). In 1969 the Organisation for Economic Cooperation and Development (OECD), an international body of 29 countries, became the first international organisation to recognise the privacy implications of the transborder data flow of personal information when its Data Bank Panel examined the privacy issues associated with digital personal information (Holvast *et al.*, 2001:1).

### 2.7.2 The 1970s

In 1970 the United States Congress passed the Fair Credit Reporting Act to protect individuals from any misuse of personal information by Credit Reporting Agencies (Rotenberg, 2001:1).

Sweden introduced its Data Act in 1973 to prevent undue encroachment on individual privacy. This Act requires registration and licensing of databases with personal information (Hussain & Hussain, 1992:153). Four years after the USA passed the Fair Credit Reporting Act, the Privacy Act and the Freedom to Information Act were passed by the United States Congress in 1974. Whereas the Privacy Act of 1974 grants citizens access to their own personal files kept by the government, the Freedom of Information Act allows citizens to access all federal agency records (Rotenberg, 2001:39,60). This was followed by the Right to Financial Privacy Act of 1978 that sought to regulate the disclosure of personal financial information to federal agencies in the USA. This Act also recognises individuals' privacy interests in their bank records, and gives them rights regarding the disclosure of these records (Rotenberg, 2001:79). In 1977, the Federal Data Protection Act was introduced in Germany to guard against any misuse of personal data during storage, communication, modification and erasure, and to prevent harm to any personal interest of the person concerned (Hussain & Hussain, 1992:153).

### 2.7.3 The early 1980s

In 1980 the Privacy Protection Act was passed in the USA. This Act establishes procedures for law enforcement seeking access to records and other information from the offices and employees of a media organisation (Rotenberg, 2001:101). On 23 September 1980, the OECD issued guidelines for privacy protection in the transfer of personal information across national borders. In developing the guidelines, the OECD worked closely with the Council of Europe, which was at that time drafting its own Convention on Privacy (Rotenberg, 2001:268). Canada passed its Privacy Act in 1982. This Act establishes rules applying to any information collected and used by government and introduces a fair information code to regulate government's handling of personal records (Holvast *et al.*, 2001:2). The United Kingdom's Data Protection Act was put in place in 1984, preventing the international transfer of personal information if it considered that information to be inadequately protected in the receiving country (Collier, 1995:42). In 1984, the USA passed the Cable Communication Policy Act to provide a strong statutory framework for the protection of television cable subscribers'

personal information. The Act incorporates the privacy principles set out in the OECD Privacy Guidelines of 1980 (Rotenberg, 2001:107).

### 2.7.4 The mid- to late 1980s

In 1985, the OECD extended its guidelines to cover transborder data flow. The Council of Europe had concluded the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981, and it came into effect in 1985. The Council negotiated the Convention in response to the rapid rise of automated data processing, and advances in computer technology that were allowing more and more records to be stored and transferred digitally (Rotenberg, 2001:297). Although there are many similarities between the OECD Guidelines and the Council of Europe Convention, the OECD Guidelines are advisory in nature and not legally binding on its members, whereas the Council of Europe Convention is legally binding on any Member State that ratifies it (Holvast *et al.*, 2001:2).

The Electronic Communications Privacy Act was enacted in the USA in 1986 as an amendment to the Omnibus Crime Control Act of 1968, to address technological advancements in communication networks and to bring electronic communication within the ambit of federal law regarding wiretapping and bugging (Rotenberg, 2001:111). Under this law, neither private entities nor government can gain unauthorised access to stored messages such as e-mail, nor can they intercept these messages (Schwartz, 1998:49). During 1988, the USA amended the Federal Criminal Code to prohibit the disclosure of video rental records containing personally identifiable information by enacting the Video Privacy Protection Act of 1988 (Rotenberg, 2001:165). In Australia, the Privacy Act of 1988 details Information Privacy Principles based on the OECD Guidelines, covering the Commonwealth (federal) public sector. Australia's Privacy Act also applies to the private sector in that it includes provisions and guidelines governing the consumer credit industry and restricts the use of tax file number information (Rotenberg, 2001:413).

At the end of the 1980s, three important areas of divergence were observed in the world's data-protection policies. The first concerned the scope: most of the European countries applied the same statutory principles to both the public and private sector. The USA, Canada, Australia and Japan, however, rejected an 'omnibus' approach, preferring to regulate only the public sector's practices and to leave the private sector governed by a few sectoral laws and voluntary codes of practice. The second difference was a disagreement about whether these laws should apply only to computerised personal data and/or also to manual record-keeping systems. Most countries chose to make no distinction, except for Sweden, the United Kingdom and Austria. The third and principal difference concerned the choice of policy instruments to enforce, oversee, and administer the implementation of the legislation. These powers range from the stricter licensing and registration regimes in force in Sweden and Britain to the more advisory and less regulatory systems headed by privacy or data-protection 'commissioners' in Germany, Canada, and Australia (Agre & Rotenberg, 1998:101).

### 2.7.5 The early 1990s

The United Nations provided ten principle guidelines for the Regulation of Computerised Personal Files concerning the minimum privacy guarantees that ought to be reflected in national privacy laws These guidelines were adopted on 14 December 1990. These guidelines mirror the OECD's eight guidelines, but set them out in slightly different ways (Rotenberg, 2001:307). The Telephone Consumer Protection Act of 1991 amended the Communications Act of 1937 in the USA. The purpose of this amendment was to prohibit any person within the USA from using an automatic telephone dialing system to make a call to any emergency telephone line or to any telephone number for which the called party was charged for the call without the consent of the called party, with specified exceptions. The Act also prohibits the use of a telephone facsimile machine, computer or other device to send an unsolicited advertisement to a fax machine (Rotenberg, 2001:178). New Zealand introduced a Privacy Act in 1993 with the object of promoting and protecting individual privacy in respect of information about individuals in accordance with the OECD Guidelines (Holvast *et al.*, 2001:1). In 1994, the Driver's

Privacy Protection Act was enacted. It requires all the States in the USA to protect the privacy of personal information contained in an individual's motor vehicle record, excluding traffic violations, license status and accidents in which the driver was involved (Collier, 1995:42; Rotenberg, 2001:188).

### 2.7.6 The mid 1990s

The Personal Data (Privacy) Bill was signed into law in Hong Kong on 3 August 1995. This resulted in a Personal Data (Privacy) Ordinance. The main international effect of the ordinance is the restriction it places on the transfer of personal data outside Hong Kong. Such a transfer of personal data that are collected, held, processed or used either in Hong Kong or by a data user whose principal place of business is in Hong Kong is prohibited unless one or more specified conditions are met (Holvast *et al.*, 2001:9).

In 1995, the European Union's Directive on the 'Protection of Personal Data' and on the 'Free Movement of Personal Data' finally emerged from the European Union's complex and drawn-out legislative process (Agre & Rotenberg, 1998:105). The European Union Data Protection Directive of 1995 establishes common rules for data protection among Member States of the European Union in order to facilitate the free flow of personal data within the European Union (Rotenberg, 2001:311). Many organisations that rely on an unimpeded flow of personal data between themselves and Europe have been particularly alarmed by the European Union's Privacy Directive (Holvast *et al.*, 2001:2). The Data Protection Directive has had, and will continue to have, an impact on the data-protection policies of countries (or states) that have not yet passed such legislation, including those outside the European Union.

The pressure on non-European Union countries stems principally from the stipulation in Article 25 that data transfers to a 'third country' may take place only if that country ensures an 'adequate level of protection'. Article 26 lists a number of derogations, among which is the provision that data may be sent to countries with 'inadequate'

protection if the data controller enters into a contract that 'adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals' (Agre & Rotenberg, 1998:109). An implementation of Articles 25 and 26 can have vast economic consequences for credit-granting and financial institutions, hotel and airline reservation systems, the direct marketing sector, life and property insurance, and for any other sector that relies on the flow of personal data across international borders (Agre & Rotenberg, 1998:109).

In 1996, the International Labour Office in Geneva compiled a Code of Practice on the Protection of Workers' Personal Data. The purpose of this Code of Practice is to provide guidance on the protection of workers' personal data when developing legislation, regulations, collective agreements, work rules, policies and practical measures. This Code does not have binding force and does not replace national laws, regulations and international labour standards (Rotenberg, 2001:364).

In the same year, the USA amended the 1934 Communications Act to the Telecommunications Act of 1996. Section 222 of the Act provides that telecommunications carriers must protect the confidentiality of Consumer Proprietary Network Information (CPNI). CPNI includes the calling patterns, billing records, unlisted telephone numbers and home addresses of service subscribers (Rotenberg, 2001:192). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by the United States Congress to combat fraud by standardising the format, use and security of electronically transmitted healthcare information. HIPAA's security and privacy standards are an important step toward building consumer confidence enabling increased electronic transactions in the healthcare industry in the USA (Hanks, 2002:1).

The unprecedented growth of communication networks and associated technologies for privacy and security has created a need for an international policy framework to harmonise national policies and promote techniques to safeguard communication networks. In 1997, the OECD adopted the Guidelines for Cryptography Policy. The Guidelines are a non-binding agreement identifying the policy goals that countries

should implement when drawing up cryptography policies at national and international levels (Rotenberg, 2001:351).

In December 1997, the European Union adopted the Directive of the European Parliament and of the Council concerning the processing of personal data and protection of privacy in the telecommunications sector (Rotenberg, 2001:339).

### 2.7.7 The late 1990s

In 1998 the Children's Online Privacy Protection Act was introduced in the USA. It prohibits an operator of a website or online service directed at children, or any operator who has actual knowledge that it is doing so, from collecting personal information from a child in a manner that violates regulations required under this title which are designed to protect such children from unlawful and deceptive practices in the collection of personal information (Rotenberg, 2001:196).

In 1999 the Financial Modernisation and Privacy Act, also known as the Gramm-Leach-Bliley Act (GLB Act) was introduced. This Act is regarded as the most sweeping legislation in the USA affecting banks and other financial institutions since the Depression in the early 1930s. The passage of the GLB Act permits banks, insurance companies and brokerage firms to operate as one entity, enabling them to offer a wider range of products and services, but with great implications for consumer privacy rights. To regulate the disclosure of consumer data among affiliates, the GLB Act requires financial institutions to give customers a Privacy Policy notice informing them of the kind of information it collects about them and how it uses that information. It also requires financial institutions to give consumers the right to 'opt out' or prevent the sale of personal data to third parties, and to develop policies to prevent fraudulent access to confidential financial information (Rotenberg, 2001:205). In brief, institutions will have to comply with standards governing how non-public personal customer information can be shared with affiliates and third parties and how disclosure of their privacy policies is carried out (Stein, 2000:121).

### 2.7.8 The 21st Century

On 23 March 2000, the Personal Data Protection Law was proclaimed by the President of Latvia. The purpose of this Law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, with respect to the processing of data regarding natural persons (Rotenberg, 2001:371). In the same year, the Czech Parliament enacted the Protection of the Personal Data Act of 2000 of the Czech Republic. This Act regulates the protection of personal data of natural persons and the rights and obligations arising within the data processing and it specifies the conditions under which personal data may be transferred to other countries (Rotenberg, 2001:382).

In Australia, the Privacy Amendment (Private Sector) Bill 2000 was passed by the Australian Parliament on 6 December 2000 and received Royal Assent on 21 December 2000. The new legislation, effective from 21 December 2001, contains amendments to the Commonwealth Privacy Act of 1988 and will regulate the handling of personal information by private sector organisations (Rotenberg, 2001:413).

On 21 July 2000, the United States Department of Commerce, responding to possible restrictions of personal data from Europe to the USA as a result of the European Union Data Privacy Directive, issued what is known as its 'Safe Harbor Privacy Principles'. The Safe Harbor programme was agreed to after the USA insisted that a voluntary approach to data privacy was better than a legislative approach. It took more than two years for the European Commission and the Department of Commerce to negotiate the contents of the Safe Harbor programme (Bureau of National Affairs, 2002h:191). Organisations in the USA acceding to the 'safe harbor' principles are seen by the USA as fulfilling the adequate protection requirement of the European Union Directive. It is interesting that the 'Safe Harbor' principles only apply to automated data and this is, in itself, a clear violation of the European Union Directive, which covers automated and manual types of data (Holvast *et al.*, 2001:14).

The Personal Information Protection and Electronic Documents Act of 2000 came into force in Canada on 1 January 2001. The Act establishes rules that govern the collection, use and disclosure of personal information in the private sector (Kirwin, 2002). The third stage of the Act will enter into force on 1 January 2004, when the law will extend to every organisation that collects, uses or discloses personal information in the course of a commercial activity within a province (Pitcher & Oorloff, 2002:1-2).

On 26 October 2001, President George W. Bush signed into law the USA Patriot Act of 2001. This Act, which arguably opens the door to invasion of privacy by the state, was introduced only days after the 11 September 2001 terrorist attacks on the World Trade Centre and the Pentagon. This anti-terrorism legislation is intended to expand the intelligence and law enforcement capability to identify and disrupt terrorist activities. The changes brought by the enactment of the USA Patriot Act will not only substantially affect individual privacy rights, but will also have broad ramifications for organisations, particularly those engaged in the provision of communications and financial services (Raul & Tyler, 2001:21).

The new European Union Directive on the protection of personal data and privacy in the electronic communications sector took effect on 31 July 2002. This new Directive introduces new rules on data retention and unsolicited commercial communications (Mason, 2002).

Thus, in today's information age, it is evident that protection of personal data transfers varies from nation to nation, as does the regulatory framework governing them. There has been marked shift in the direction of a global standard for information privacy modelled on the provisions of the European Union (Rudraswamy & Vance, 2001:133). It is clear that the European Union's 1995 Data Protection Directive constitutes the rules for the increasingly global character of data-processing operations. Its effect on countries outside the European Union is principally a penetrative one. The increasing global interdependence means possible consequences for those organisations that rely

upon the unimpeded flow of personal information, and which cannot claim to protect the data of consumers, clients and employees in ways that match the European standard (Agre & Rotenberg, 1998:111). In an interdependent world, the policy efforts of the Europeans carry externalities that force other countries to pursue policies that they would otherwise oppose or avoid. The alternative is to bear the costs of maintaining a different public policy. In addition, the general pressures to conform have increased as more and more countries have joined the 'data-protection club'. There is an increasing perception that adequate privacy protection is a necessary condition for being on the global information highway (Agre & Rotenberg, 1998:112).

As the global marketplace continues to expand, organisations face increasingly strict privacy and data protection regulations in a growing number or countries around the world. Many governments are following the lead of the European Union by developing omnibus privacy legislation to address public concerns about the protection of personal information (Pitcher & Oorloff, 2002:1). Regulatory frameworks with laws or a lack of laws in different countries can pose serious problems for transnational and multi-national organisations conducting business world-wide. This may have far-reaching social and ethical implications, particularly when those organisations fail to comply with the existing regulations that protect the privacy of the individuals or the entities involved. It is therefore important for multi-national organisations to understand the regulatory environment in different countries. This is also relevant when multi-national organisations focus on globalisation in order to diversify and expand potentially new markets to gain competitive advantage (Rudraswamy & Vance, 2001:128). Obviously South Africa can draw on the experience of Western countries. Whatever privacy laws the international community adopt, there will be strong and perhaps irresistible pressure on South Africa to follow suit.

## 2.8 SUMMARY

This chapter has introduced the concept of privacy from a constitutional perspective. In the Bill of Rights, Chapter 2 of the Constitution, South African citizens are guaranteed

(among other things) the right to privacy and the right to access of information. The Promotion of Access to Information Act 2 of 2000 was promulgated to give effect to the constitutional right of access to any information held by the state, as well as any information that is held by another person and that is required for the exercise or protection of any rights. However, this Act excluded private sector portions and data protection provisions. This led to a request from the Minister for Justice to form a Committee (Project 124) to investigate the privacy and data protection issue with the aim of improving existing legislation and adding new legislation. Because of the marked shift toward a global standard for information privacy, the chapter has also provided a brief historic overview of privacy and data protection in the international environment.

Several forces are working toward a global convergence of the conceptual content and legal instruments of privacy policies. These forces include shared technology and a well-networked global policy community. One problem in dealing with privacy issues is that not everybody is concerned with the same issues, at the same time, to the same extent, or in the same way, making legislation to protect privacy very problematic. Legislating this area is even more difficult in an international situation, and when one attempts to regulate the issue across different countries, as is currently the case.

The chapter concluded that South Africa has to adopt privacy and data protection legislation because of pressure from the international community and the fact that data privacy is becoming a global concern with transnational implications. South African organisations cannot ignore European Union privacy laws, since these laws have an impact outside the European Union, affecting South Africa as well.

The next chapter focuses on data protection as a privacy issue. Chapter 3 will addresses the information privacy issues surrounding the collection, use and dissemination of consumers' personal information in a commercial environment, as well as the responsibility of organisations to limit media intrusion and develop privacy practices and policies.