Chapter 1
Identifying problem and setting parameters

CONTENTS

1 DATA PROTECTION: LEGAL RESPONSE TO A PRESENT-DAY PROBLEM

1.1 Collection of personal information – not a new phenomenon

The collection of information on individuals is not a new phenomenon. In fact, record keeping on individuals is as old as civilisation itself. The Roman Empire, for example, maintained an extensive

system of taxation records on its subjects, who were identified through census taking.[1] Similarly, William I of England (William the Conqueror) decreed that a variety of information was to be collected on his subjects and in 1086 his scribes began to keep records in the *Domesday Book*.[2]

Another (infamous) collection of personal information was the files of the SD (*Sicherheitsdienst*) of Nazi Germany. When the German army invaded Denmark, Norway, the Netherlands, Belgium, Luxemburg and France in 1940, the Nazis found advanced systems of paper records on the citizens of all these countries. These records were analysed by the SD to determine who was Jewish, of Jewish descent or a Jehovah's Witness, who voted for leftist parties such as the Socialists or Communists, who were vagabonds (Romanies or gypsies), who contributed money to causes not favoured by the Nazis (Catholic and Protestant charities, liberal colleges and universities) and who were members of secret societies such as the Freemasons.[3] The result of these personal data analyses is now well known.[4] According to Madsen, "upon invading another country, the capture of personal information records that had political significance was the first priority of the SD. Nations that maintained advanced systems of records had, in reality, done the SD's work for them already".[5]

---

1 We read of such a census in the Bible when Joseph and Mary went to Bethlehem to have their names recorded in the population register (Luke 2: 2–4). For more information on the Roman Empire's census taking activities, see Madsen *Personal data protection* 6–7. Bennett *Regulating privacy* 18 points out that historical research has traced the notion of a system of personal records to most of the ancient civilisations of the Far and Near East, Central and South America and the Mediterranean.

2 See also Madsen *Personal data protection* 7.

3 Madsen *Personal data protection* 23. Madsen explains that "information was recorded on cards stored in immense cylindrical filing cabinets, each with a capacity for five thousand cards. The cabinets revolved automatically and individual cards could be extracted by pushing buttons. This was probably the first automated information retrieval system albeit a crude one. The next logical step for the SD, had their existence continued, would have been to adopt the early computer-based punched card technology to store this type of information".

4 "Jews and those of Jewish descent, Jehovah's Witnesses, seminary students, gypsies, the mentally retarded, Socialists, Communists, pacifists, Liberal Republicans, Catholic Action and Catholic Youth members, Protestant theologians and homosexuals were rounded up by the SD's sister service, the Gestapo, for shipment to concentration camps and in most cases to their deaths" (Madsen *Personal data protection* 23).

5 Madsen *Personal data protection* 23. These experiences explain why European countries and the USA today view the threats posed by large scale collection of personal information from a different perspective (see Madsen *Personal data protection* 2).

With rapid population growth, the emergence of present-day society and the extension of the powers of central governments, more and more reasons – political, economical and social – arose for governments and private persons to collect information on other persons, the result of which was the creation of a whole new information-collecting industry.[6] Information, including personal information,[7] has become such a necessary and valuable commodity that the era that we live in has become known as the "information age" and the post-industrial society as the "information society".[8]

Not only has the quantity of information being collected increased; the quality of the collection has also changed. More sensitive and potentially prejudicial information on matters such as people's finances, health and employment history is collected.[9]

Thirty years ago the Privacy Protection Study Commission (PPSC)[10] described the dramatic changes that had taken place in the collection of personal information in the USA over the previous hundred years.[11] The PPSC indicated that records dating from a hundred years ago revealed little about average Americans; at the most they indicated when people died, what the date and place of their birth were, whether they owned land, and if so, how they had obtained the title to it. Three-quarters of the adult

6 Bennett *Regulating privacy* 19; Neethling *Privaatheid* 11.

7 Personal information is used in the sense of information that can be related to a person (see below par 1.7.1).

8 See Bennett *Regulating privacy* 16–17; Lloyd *Information technology law* xxxv; Cate 1995 *Iowa L R* 431, 439–440; Seipel "Computers and information power" 8; Martin *Bits, bytes and big brother* 19. But see Goldman "Privacy and individual empowerment" 97 who indicates that the "information age" is evolving in the "interactive age" because the consumer is more and more engaged in a variety of activities by the new communications technologies.

9 Bennett *Regulating privacy* 19.

10 A temporary body established by the USA Privacy Act of 1974 to study, *inter alia*, data banks, automated data processing programs and information systems of governmental, regional and private organisations in order to determine the standards and procedures in place for the protection of personal information. Also see ch 2 par 4.2.5.

11 Privacy Commission Report 3–4. Although this study was based on the position in the USA, its findings are equally applicable to present-day South Africa. Issues such as privacy protection and transborder data flows were initially considered by developing countries to be "the luxury of the developed post-industrial society" (see Ennison 1984 *Int Bus L'yer* 163, 164). Today these are burning issues in South Africa and many other developing countries. Also see Schwartz 1992 *Hastings LJ* 1321, 1329 *et seq*.

population worked for themselves on farms or in small towns and school attendance was not compulsory. No national military service was required and few programmes brought individuals into contact with the federal government. Local governments kept some records relating to taxes, criminal records, business regulation and public relief of the poor or insane. However, these record-keeping practices were limited and local in nature. The churches probably kept the most complete records, recording births, baptisms, marriages and deaths. Similar records were kept by town and county officials. Merchants and bankers maintained financial accounts for their customers and when they extended credit, it was on the basis of personal knowledge of the borrower's circumstances. Few individuals had insurance of any kind and a patient's medical records were likely to exist only in the doctor's memory.

While the PPSC was carrying out its study in the 1970s, three-quarters of all Americans lived in cities and only ten percent of the population were self-employed. Education was compulsory. Most Americans did at least some of their buying on credit and most of them had some form of life, health, property, or liability insurance. Institutionalised medical care was almost universally available and government social services programmes reached deep into the population along with government licensing of occupations and professions, Federal taxation of individuals and government regulation of business and labour union affairs. According to the PPSC, a significant consequence of this change in the variety and concentration of institutional relationships with individuals was that record keeping as it related to individuals covered almost everyone and influenced everyone's life.

Everybody's creditworthiness, ability to obtain insurance, medical care needs, employment and educational history and ability to qualify for social services were evaluated on the basis of recorded information in the files of one or more organisations. Each of those relationships required individuals to divulge personal information.

A further dramatic change was the substitution of records for face-to-face contact in these relationships. It became commonplace for individuals to be asked to divulge information about themselves for use by unseen strangers who made decisions about them that directly affected their everyday life. Because so

many of the services offered by these organisations had come to be considered necessities, individuals had little choice but to supply the required information. Since the organisations could no longer rely on personal knowledge of the individual when making these decisions, they increasingly desired more detailed information to enable them to distinguish between individuals in making what were referred to as "fine-grained decisions".

Over the past thirty years even more far-reaching changes have taken place, mostly due to the spectacular developments in the field of information technology.

1.2 Influence of computer and information technology on collection of personal information

The advent of computers has played a crucial part in making information a valuable commodity and has influenced the collection of information as to both quantity and quality.[12] Computers are able to store vast amounts of information (in the form of raw data)[13] relatively easily, cheaply and for almost indefinite periods.[14] Furthermore, they are able to process and disseminate such information at incredible speeds. The end result of such processing is often the creation of new information that forms the basis of decision making, by either humans or – frequently – the computer itself.

The development of new telecommunications technology, linking computers in networks (principally the Internet)[15] and enabling the transfer of information between computer systems, has made information

12 Computers have been used since the mid-1950s to process information. For fifty years before that, data were processed with the aid of punched cards (Davis *Computer data processing* 1). The first computer that was commercially used, the UNIVAC 1, was installed in 1951 at the United States Bureau of Census (Davis *Computer data processing* 8).

13 The two concepts "information" and "data" are often used interchangeably (as is done in this thesis). For a detailed analysis of the difference between the two concepts, see par 1.7.1.

14 Flaherty *Surveillance societies* 2; Schwartz 1992 *Hastings LJ* 1321, 1334–1343.

15 The Internet was preceded by ARPANET, a network sponsored by the Advanced Research Projects Agency (ARPA) of the US Defence Department, in 1969. During the 1970s and 1980s the Internet was mainly used by the academic community. Commercial usage of the Internet was only allowed in 1991. An (continued...)

increasingly important, and boosted the collection and use of information. Initially, computers were used to expand and automate existing informational practices. Computers were mainly used by governments and large institutions, such as banks. All the information of a particular organisation was stored on a handful of stand-alone computers (also called "mainframes").

With the development of personal computers linked by communication networks, it is no longer necessary for an institution to keep all its information on a particular machine, at a particular place or even in a particular country.[16] Networks enable more users to gain access to a wider range of personal information. Different organisations keep financial, medical, educational or employment records on individuals for a variety of purposes. In theory all of this information can be shared by different computer users across networks.[17]

Some of the risks posed by the use of computers to process personal information already existed with a system of manual administration of data, but these risks are greatly increased when the data are handled automatically. The risks inherent in the processing of personal information, be it manually or automatically, are that the data may be:[18]

- ❒ inaccurate, incomplete or irrelevant
- ❒ accessed or disclosed without authorisation
- ❒ used for a purpose other than that for which they were collected
- ❒ destroyed

15(...continued)
important technical innovation was the development of the WWW in 1992 by Tim Berners-Lee. It uses hypertext to create links between documents (see further Lloyd *Information technology law* 7–10). Today, it is estimated that there are at least one million websites. For risks posed to privacy by the Internet, see Buys *Cyberlaw* 365 *et seq*; Hofman et al *Cyberlaw* 43 *et seq*.

16 The notion of information that is stored in a file has therefore also become outdated. "Today data is scattered in (in various locations) and thus it is no longer found in a single organised set (a file)" (Benyekhlef "Dematerialized transactions" 110).

17 Lloyd *Information technology law* xxxviii – xxxix.

18 Neising & de Houwer *Transborder flow of personal data* 16.

However, the following additional risks are the result of the very nature of automatic processing:[19]

- ❒ the difficulty of checking the contents of storage systems, because information is stored in a form which is not immediately intelligible
- ❒ the unlimited amount, range and nature[20] of the data stored
- ❒ expanded possibilities of storing, comparing, linking,[21] sharing,[22] selecting and accessing[23] personal data

Miller[24] describes the threat posed by computers succinctly:

> The computer with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn our society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer.

1.3 New threats to privacy

19 Neising & de Houwer *Transborder flow of personal data* 16; McQuoid-Mason *Privacy* 195–196; Faul *Bankgeheim* 524.

20 The data may be of a very personal and even intimate nature.

21 The centralisation and coupling of data collected from various sources and for various purposes are made possible due to the possibilities of linking several data banks to each other, thus creating one single file and several national and international data banks.

22 Data can be shared by different data users. The South African Insurance Association eg, maintains a claims database for all its members. The purpose of such a shared database is to combat fraud. E-governance, where the government has one database for all government departments, is another example of data sharing.

23 The speedy, cheap and untraceable access to large quantities of personal data gathered in various places and at various moments enables the composition of an individual's profile that has an influence on decisions concerning the individual's qualifications, credit eligibility, health, insurance, consumption patterns, social security and employment, etc.

24 Miller Statement to the US Congress Senate Committee on the Judiciary, 1967 (as quoted in 1972 *Int Soc Sci J* 429 fn 1).

In every generation there are new technological inventions that create an increased threat to the privacy of persons.[25] Apart from apparently wrongful processing of data (for example, without a legitimate reason to justify such processing), this generation will have to deal with more subtle data processing issues, such as data matching, profiling /automated decision making, data mining, smart cards and "cookies". Since reference will be made to some of these practices in the subsequent discussions of the data protections laws, they are described at the outset.

Data matching: Data matching, also called computer matching or record linkages, entails the comparison of the records of different agencies or institutions by using a common denominator, such as a social security number, to find persons who may be included in more than one file, in order to determine, for example, whether ineligible persons are receiving benefits under a government program. The aim of these programs is usually to eliminate fraud, waste and abuse from government programs, but a side effect could be that the government builds up dossiers about individuals.[26]

Profiling: In computer profiling (also referred to as automated decision making), record systems are searched for a specific combination of historical elements, the so-called profile, in order to make a judgment about a particular individual based on the past behaviour of other individuals who appear statistically similar, in the sense that they have similar demographic, socioeconomic, physical or other characteristics.[27] Bygrave[28] defines profiling as "the inference of a set of characteristics, (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other

25 In 1890, Warren and Brandeis, two Boston lawyers, complained that "[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual... the right 'to be let alone.' Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops". See Warren & Brandeis 1890 *Harv LR* 193 *et seq*.

26 Flaherty *Surveillance societies* 344. See also Borking "Privacy technology" 97; Madsen *Personal data protection* 12; Turkington & Allen *Privacy law* 313.

27 Borking "Privacy technology" 97. Also see Bennett *Regulating privacy* 19 and ch 3 par 4.2.4.8. Bygrave *Data protection law* 302 correctly points out that profiling is closely tied up with discrimination, in the sense that it involves taking (or not taking) action (often exclusionary) on the basis of perceived differences between persons or classes of persons.

28 Bygrave *Data protection law* 301.

persons/entities in the light of these characteristics. The set of characteristics will typically relate to the behaviour (actual or expected) of a person/entity". As Bygrave points out, profiling as such is not a new phenomenon, but what is new is the increasingly extensive, systematic use by organisations of relatively formalised and sophisticated profiling practises for a variety of control purposes.[29]

The profiling process consists of two components: first the creation of a profile, and second the process of treating persons in the light of this profile. The creation or inferring of a profile consists of processing data in search of patterns, sequences and relationships, whereas the application stage involves making a decision about a person based on the profile.[30] As Bygrave explains, "profiles are essentially assumptions based on probability equations".[31] The quality of a profile is obviously dependent on the quality of the data (in terms of correctness, relevance, etcetera) put into the profile. A real danger with profiling is that unfair or unwarranted assessments can be made about data subjects.[32]

Profiling is used for various purposes, such as direct marketing of goods and services, credit assessment, law enforcement and crime control. Another use is to provide cost-effective health care, because profiling can help to identify persons who are likely to develop particular health disorders.[33]

Although data matching and profiling are two distinct processes, it should also be recognised that profiles can be generated, reinforced or modified on the basis of data matching, and data matching can be designed and initiated on the basis of profiles.[34]

Data mining: With so-called "knowledge discovery in databases" or "data / information mining", new

29 Bygrave *Data protection law* 301.

30 For a complete description of the profiling process, see Bygrave *Data protection law* 302 *et seq*.

31 Bygrave *Data protection law* 309.

32 Bygrave *Data protection law* 310.

33 See further Bygrave *Data protection law* 304–305.

34 Bygrave *Data protection law* 302.

information is discovered in old, existing databases. Existing databases are analysed or "mined" by means of new search techniques, revealing previously hidden information.[35] Sometimes new databases are created in order to mine them for new information – the process where an organisation collects information from disparate sources and loads these data into a central integrated database for subsequent analysis and (re)use is called **data warehousing.**[36]

Smart card: A "smart card" is a small electronic device about the size of a credit card that contains an integrated circuit ("chip") for memory purposes. It is used for a variety of purposes, such as to contain a patient's medical records, store digital cash, or store identifying information.[37] The smart card may provide improved security and privacy, but it could potentially be misused. If the information on the card is relayed to a database and linked to other information, a dossier on all aspects of a person's life – financial, medical, purchasing behaviour, or travel patterns – can be created.[38]

Cookies: The fact that personal computers are increasingly connected to the Internet even makes it possible for individuals' personal computers to collect information on them and to pass it discreetly on to companies eager to learn about their shopping habits and other useful personal information. One way of collecting information via the Internet is through the use of "cookies" – bits of data that are stored on an individual's computer when he or she visits a particular website. This enables websites to keep a record of users of their sites. Internet service providers also have the ability to keep track of the websites that the Internet user visits and the software that he or she downloads.[39] Cookies may contain

35 See Gardeniers, Van Kralingen & Schreuders "Privacyaspecten van informatie-mijnbouw" 69.

36 Bygrave *Data protection law* 306.

37 See also Hofman *et al Cyberlaw* 47; Meiring *Betalingstelsel* vii.

38 Borking "Privacy technology" 95. See also Hofman *Cyberlaw* 47–48.

39 So-called "ET software" is another example of even more invasive software. *Time Magazine* (31 July 2000 36–43) discussed this new kind of software, referring to it as "software that commandeers your computer to spy on you" (at 38). According to *Time Magazine*, when one downloads free software from a specific company, designed to help one with on-line shopping, this software not only does useful things like giving recommendations about products while one is shopping on-line, it also does other unpleasant things:

> This software plants itself in the depths of your hard drive and, from that convenient vantage point, starts digging up information. Often it's watching what you do on the

(continued...)

personalised information in relation to the website that was visited, such as login codes, passwords, credit card numbers or a list of shopping items.[40] Where personal information is contained in the cookie which is sent back to the website owner, the privacy of the computer user (data subject) is infringed.

Spam: Sending unsolicited e-mails (referred to as junk mail or "spam") is also considered an infringement of the privacy of the persons whose e-mail addresses are used without their permission.[41] The e-mail addresses used by the "spammers" are obtained by buying them from on-line businesses or by "mining" other sources, such as messages posted on mailing lists, from newsgroups or from domain-name registration data. An e-mail address contains personal information and when an e-mail address is freely circulating on countless directories, the data subject's privacy is being infringed. "Spam" is used by direct marketing organisations that are interested in advertising their product to the broadest possible circle of potential buyers in the cheapest possible way. Data subjects' privacy can be protected by allowing them to either "opt-in" or "opt-out" of inclusion on a direct mailing list.[42]

1.4 Extent of collection of personal information

In order to illustrate the present extent of the processing of personal data and the threat this poses to the individual, it is necessary to refer to the most important data controllers. Data controllers[43] could come from either the public or the private sector. **Public controllers** process data on a wide range of topics, owing to the state's numerous activities and functions. These would include data on civil servants

39(...continued)

> Internet. Sometimes it's keeping track of whether you click on ads in software, even when you are not hooked up to the Internet. ... These programs are known as E.T applications because after they have lodged in your computer and learned what they want to know, they do what Steven Spielberg's extraterrestrial did: phone home. That may be the most paranoia-inducing part. E.T applications use your Internet connection to deliver espionage briefings on you, often without you realizing it is happening.

40 Kaspersen "Data protection and e-commerce" 138.

41 EPIC *Privacy and human rights* 59; Kaspersen "Data protection and e-commerce" 141; Buys *Cyberlaw* 381 *et seq*.

42 See further ch 6 par 2.4.4 where direct marketing and the "opt-in" or "opt-out"options are discussed.

43 For a definition of the term "data controller", see par 1.7.3

as employees; conscripts in the defence force; pupils and students at educational institutions (such as schools, colleges, technikons and universities); suspects, accused persons and prisoners at the police and correctional services; taxpayers at the office of the South African Revenue Service; recipients of welfare at social services; and data on all individuals derived from census reports and population registration figures. The processing of these data is usually justified by their public importance[44] and the storage and use of the data are generally essential for the proper functioning of the government and effective national planning. Since individuals may be compelled by legislation[45] to furnish information on themselves to the state, the state controls this unique source of information directly.[46]

Private controllers: Credit bureaus are important private data controllers. The main object of credit bureaus is to collect and furnish information concerning the creditworthiness of people. However, their activities are not always confined to this subject and other personal and even intimate facts such as drinking habits, health, characteristics, reputation, extra-marital relationships, political and religious convictions, criminal records, race, sexual preference, etcetera are often included in the data files. The result is that credit bureaus may be capable of disclosing a complete record not only of someone's

44 See *S v Bailey* 1981 4 SA 187 (N) 190.

45 Acts that allow the state to process personal data in South Africa include, eg, the Statistics Act 6 of 1999, the Income Tax Act 72 of 1986 and the Identification Act 68 of 1997. The Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 which will replace the Interception and Monitoring Prohibition Act 127 of 1992, requires of service providers to provide a telecommunication service which has the capability to be intercepted and to store communication related information (Act 70 of 2002 s 30). Communication related information refers to switching, dialling or signalling information that identifies the origin, destination, termination, duration, equipment used and location of the user (where applicable) in respect of each indirect communication generated or received by a customer or user of equipment, a facility or service provided by the telecommunication service provider. An indirect communication means the transfer of a message in the form of eg speech, music, data, text, visual images, signals or radio frequency spectrum (Act 70 of 2002 s 1). The service provider therefore acts, as it were, as the processor for the state as data controller. A direction to intercept communications, or to provide communication related information may be issued by a designated judge if the judge is satisfied on the facts alleged that there are reasonable grounds to believe that certain grounds are present (see eg s 16(5)). The public interests that are the object of protection are the prevention or detection of serious crime, public health or safety and national security or compelling national or economic interests of the Republic.

46 Neethling *Persoonlikheidsreg* 324.

creditworthiness, but also of his entire personal life.[47]

Other significant private data controllers are banks and other financing institutions that process data on their clients' financial status; private detectives that process data on every aspect of a person's life;[48] employers who process a wide range of data on their employees;[49] the insurance industry that processes personal data relating to insurance risks posed by their clients and prospective clients;[50] the medical profession (medical practitioners, dentists, psychiatrists and psychologists) that processes data on the health of patients; and voluntary associations (such as churches) that process personal data on their members. There are also direct marketing agencies which make and sell lists of the addresses of individuals (often connected to other personal data), usually for advertising purposes, and researchers who process statistical data on groups of people.[51]

1.5 Interests threatened by processing of personal information

Alexander Solzhenitsyn wrote as follows:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions ... There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become

47 Neethling *Persoonlikheidsreg* 323 indicates that credit bureaus acquire their information from different sources, such as their clients, eg commercial banks and financing houses which provide information on their own clients' occupations, incomes and general creditworthiness. Information can also be obtained from commercial concerns selling on credit who may report on their clients' records regarding payment of their obligations. Another important source is official records, from which facts concerning arrests, litigation, sentences, insolvencies, mortgage bonds, births, marriages, divorces and deaths may be learned. Newspaper reports are an obvious but highly unreliable source. Owing to the fact that it is often difficult to identify data subjects positively from newspaper or court reports, the real possibility exists that data reports on persons in credit bureaus may contain misleading or incorrect information.

48 This may include very personal and intimate information on a person's health, sexual activities, movements, friends, associates etc.

49 Such as name, address, date of birth, dependants, marital status, qualifications, remuneration, etc.

50 Eg in the case of a life insurance policy, information on the health of a person and even his or her family members.

51 See in general Neethling *Persoonlikheidsreg* 322–325.

> visible, the whole sky would look like a spider's web... They are not visible, they are not material, but every man is constantly aware of their existence ... Each man, permanently aware of his own visible threads, naturally develops a respect for the people who manipulate the threads.[52]

Solzhenitsyn is expressing the instinctive discomfort that individuals experience once they realise that millions of little bits of personal information on them are "out there" – collected and stored by frequently nameless and faceless persons or organisations, intent on using such information for unknown purposes. The argument is sometimes advanced that if one has nothing to hide, it does not matter that other persons possess personal information about one. Philips[53] answers this argument convincingly:

> Of course we have nothing to hide, but that is not the point. Even if someone has nothing to hide, she has a great deal to lose. One's autonomy, sense of anonymity and the right to go about ... [one's] business unmolested are severely challenged. Even if one has nothing to hide, surveillance will subtly alter a person's behaviour. Take away ... [peoples'] privacy and you take away their dignity and their control over their life.

It is generally accepted that the processing of personal information primarily poses a threat to a person's privacy.[54] Another interest that is often threatened is identity,[55] which is infringed upon when incorrect

52 *Cancer Ward* (1968) as quoted by Bennett *Regulating privacy* 30–31. According to Selmer "Data protection policy" 23 "the fear of tyranny lies at the bottom of all data protection legislation. It was George Orwell who started the movement. Without the popular fear of Big Brother, there would have been no data protection legislation".

53 Philips 1997 *U New Brunswick LJ* 127, 132.

54 Eg, in the USA, in enacting the Privacy Act of 1974, Congress found (s 2(a)(1) Pub L 93–579) that "the privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information" and in the UK, the Lindop Committee on Data Protection declared that "privacy is the starting point of our enquiry" (see *Report of the Committee on Data Protection* 28). According to the EU Data Protection Working Party's report *Data Protection Law and the Media* 4, "[d]ata protection comes within the scope of the protection of private life guaranteed under this article [article 8 of the European Convention for the Protection of Human Rights]". Cannataci *Privacy and data protection law* 25 says: "It would be very difficult, if not downright impossible, to discuss data protection law without also discussing the notion of privacy." Also see Bennett *Regulating privacy* 23; Blume 1992 *Computer/L J* 399; Flaherty *Surveillance societies* xiii; Hondius *Emerging data protection* 2; Neethling *Privaatheid* 11; Trubow 1992 (continued...)

or misleading information relating to a person is processed.[56]

It has often been said that privacy is difficult to define, because it means different things to different people.[57] Traditionally, privacy is defined "as the right to be let alone". This definition was made famous in 1890 by two American lawyers, Samuel Warren and Louis Brandeis.[58] With the emergence of information technology the need arose for this definition to be adapted and another American, Alan F Westin, reformulated the definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[59] This claim to self-determination is indeed, as contended by Neethling, the essence of a person's interest in privacy.[60] Today, these two basic ideas of privacy as the right to be let alone and

54(...continued)
NW J Int L & Bus 159, 161. See further Bygrave 2001 *UNSWLJ* 277, 282; *Data protection law* 125 *et seq*.

55 See ch 7 par 2.3.2.1. Neethling defines identity as "a person's uniqueness or individuality which identifies or individualises him as a particular person and thus distinguishes him from others" – Neethling, Potgieter & Visser *Neethling's law of personality* 39; Neethling *Persoonlikheidsreg* 44. It must, however, be pointed out that this interest is included under the concept of privacy in American tort law, a viewpoint accepted by certain South African authors, such as McQuoid-Mason *Privacy* 201–216 and Burchell *Delict* 208–209. See ch 7 par 2.3.2.2.

56 Other personality interests may also be relevant, such as a person's good name or *fama* which is infringed through the communication of defamatory data, and dignity which is violated by insulting personal data – see Neethling *Persoonlikheidsreg* 326 fn 46. For an analysis of other values and interests associated with privacy, see Bygrave *Data protection law* 133 *et seq*.

57 See Miller *Assault on privacy* 25; Neill "Privacy" 3–4; Anderson "American privacy law" 149; *Bernstein v Bester NO* 1996 2 SA 751 (CC) 787–788. Young *Privacy* 2 observes that "[p]rivacy, like an elephant, is more readily recognised than described".

58 Warren & Brandeis 1890 *Harv LR* 193, 195 (see ch 2 par 2.1.1.) They borrowed the expression from Michigan Supreme Court Justice Cooley, who used it in the 1800's in his *Treatise on the law of torts* 29: "Personal immunity. The right to one's person may be said to be a right of complete immunity: to be let alone" (see Turkington & Allen *Privacy law* 51).

59 Westin *Privacy and freedom* 7. In this thesis Neethling's definition is used as point of departure. Neethling, Potgieter & Visser *Neethling's law of personality* 36 defines privacy as "an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy". See also Neethling *Persoonlikheidsreg* 39–40 and see further ch 7 par 2.3.2.1.

60 Neethling *Persoonlikheidsreg* 38–39 fn 329. See also *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271–272.

the right to control personal information form, according to Blume, the core of data protection.[61] It stands to reason that without control over his or her personal information, privacy will greatly diminish and may ultimately be lost.[62]

1.6 Data protection: legal response to threat posed by processing of personal information

In response to the problem of the invasion of the individual's privacy by the processing of personal information, many countries have adopted "data protection" laws.[63] This term originated from the German term "Datenschutz".[64] According to Bennett,[65] "data protection" is a technical term that refers to a "group of policies designed to regulate the collection, storage, use and transmittal of personal information". Hondius[66] describes data protection as "the body of law which secures for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms and in particular his right to privacy, with regard to automatic processing of personal data relating to him".[67] According to Bygrave data protection need not always involve legal measures. Although it has, since the 1970s, been linked to a type of legislation, it has now achieved a level of generality which goes beyond such legislation. He defines data protection as a set of measures (legal and/or non-legal) aimed

61 Blume 1997 *Int R L Computers & Tech* 193, 195. Also see Bygrave 2001 *UNSWLJ* 277, 279–281.

62 See further Bygrave *Data protection law* 125 *et seq*.

63 See Schwartz 1991 *Am J of Comp L* 618, 619; Flaherty "Data protection and national information policy" 29; Bygrave *Data protection law* 93 *et seq*.

64 However, many countries, including the USA, prefer to use the term data or information privacy, rather than data protection, because data protection sounds esoteric and means little to the average citizen – see Bennett *Regulating privacy* 23. According to Schwartz 1992 *Hastings LJ* 1321, 1374 the name "data protection law" is a bit of a misnomer, since data protection law does not merely seek to guard data, but also attempts to safeguard the individual's interests.

65 Bennett *Regulating privacy* 13. See Banisar & Davies 1999 *J Mar LR* 1, 15–111 and EPIC *Privacy and human rights* 97–382 for an overview of data protection laws world wide.

66 Hondius 1983 *Neth Int LR* 103.

67 Also see Gellman 1994 *Gov Inf Q* 245, 246 according to whom data protection "focusses attention more precisely on laws, policies, and practices that affect the collection, maintenance, and use of personal information about individuals".

at safeguarding persons from detriment resulting from the processing (computerised and/or manual) of information on them, and embodying a group of principles on the processing of personal information.[68] In this study data protection means the legal protection of a person (called the data subject) with regard to the processing of data concerning him- or herself by another person or institution.[69]

The first data protection legislation was adopted in 1970 in the German state of Hesse, and in 1973 Sweden enacted the first national data protection law, followed by the United States in 1974, West Germany and Canada in 1977, France, Norway, Denmark and Austria in 1978, Luxemburg in 1979, New Zealand in 1982, the United Kingdom in 1984, Finland in 1987, and Ireland, Australia, Japan and the Netherlands in 1988. Today almost all western countries have either adopted data protection legislation, or are considering such legislation.[70] In fact, many countries have already revised their first data protection laws or have adopted completely new, second generation data protection laws.[71]

1.7 Key terms in data protection law

In order to clarify the discussion that follows, it is necessary to describe some of the key terms at the outset.

---

68 Bygrave *Data protection law* 21–22. Data protection should not be confused with data security. Whereas data protection aims to protect the privacy of persons against data processing, data security protects the interests of data controllers, processors, and data users of all kinds of data. Data security aims to ensure that data are processed in accordance with the expectations of those who steer or use a given information system (Bygrave *Data protection law* 22). See also ch 6 par 2.2.9 on the data protection principle of security and confidentiality.

69 Neethling *Persoonlikheidsreg* 321.

70 The following countries had data protection laws in place at the end of 2002: Argentina, Australia Austria, Belgium, Brazil, Bulgaria, Canada, Chanel Islands, Czech Republic, Chile, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, (South) Korea, Latvia, Lithuania, Luxemburg, the Netherlands, New Zealand, Norway, Peru, Portugal, Poland, Portugal, Russia, San Marino, Slovakia, Spain, Sweden, Switzerland, Taiwan, the United Kingdom, the United States of America. Countries that were in the process of considering data protection laws include Malaysia, Thailand, Turkey and the Ukraine (see EPIC *Privacy and human rights* 97 *et seq*).

71 Eg, the Netherlands adopted their second generation data protection law in July 2000 and the United Kingdom adopted theirs in 1998. On "generations" in data protection laws, see also Bygrave *Data protection law* 87–88.

1.7.1 Data, information and personal information

The two concepts "information" and "data" are often used interchangeably. However, according to certain authors, the two concepts are strictly speaking not the same. These authors describe data as unstructured facts or raw material that needs to be processed and organised to produce information, whereas information refers to data that are organised, structured and meaningful to the recipient.[72] Bygrave defines information as "a human cognitive product that depicts (informs us about) a set of phenomena for a given set of purposes".[73] In this thesis these two concepts are used interchangeably, since in practice it is difficult to maintain a distinction between them and in most legal contexts it is also unnecessarily pedantic to maintain such a distinction.[74]

Personal information is used in the sense of information (or data) that can be connected to a person. It is usually defined as information relating to, and permitting identification of, individuals or persons.[75]

1.7.2 Data processing

Processing of data includes any operation performed upon personal data, such as the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, blocking, erasure or destruction of such data.[76] Traditionally, there has been a distinction in data protection laws or international instruments between (limitations on) collection, use, and disclosure of data. This does not detract from the fact that they are part and parcel of the concept of data processing.

---

72 See Davis *Computer data processing* 43; Eiselen *Reg op privaatheid in die inligtingsera* par 2. Also see Van der Merwe *Computers and the law* xv–xxii, 136–137; Geldenhuys *Regsbeskerming van inligting* 11–74; 1997 *THRHR* 254, 263 fn 47; Sieber "Emergence of information law" 1, 9 *et seq*.

73 Bygrave *Data protection law* 20.

74 See Bygrave *Data protection law* 20.

75 Bygrave *Data protection law* 2.

76 See eg Dir 95/46/EC a 2(b).

1.7.3 Parties involved: data controller, data processor, data subject, data user, third party

A **data controller** (also referred to as a data medium,[77] or responsible party[78]) is the natural or juristic person, public authority, agency or other body which determines the purposes for which and the means by which the data are processed.[79] A data controller could use a **data processor** to do the processing on its behalf. The data processor is then the person who actually carries out the processing.[80] The **data user** (or recipient[81]) is a person who receives data and applies them for various purposes.[82] The **data subject** (*betrokkene*[83]) is the identified or identifiable person whose personal data are processed, in other words, the person to whom the data relate.[84] Sometimes a third party is also distinguished. The **third party** is any party other than the data subject, the data controller, the data processor, or any person under the direct authority of the controller or the processor.[85]

2 PARAMETERS OF STUDY

The extent and seriousness of the threat posed to persons by the processing of personal data makes it evident that a legal response is necessary. Since the common law in South Africa, as will be

77 Neethling *Persoonlikheidsreg* 321.

78 Called a *verantwoordelijke* in the Dutch Wet Bescherming Persoonsgegevens (WBP) (see ch 5 par 4.3.3).

79 See eg Dir 95/46/EC a 2(d) which defines a "controller" as meaning "... the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Also see Bygrave *Data protection law* 21.

80 Bygrave *Data protection law* 21. In the UK Data Protection Act of 1984, a processor was called a computer bureau.

81 In the Dutch WBP (see ch 5 par 4.3.3).

82 Bygrave *Data protection law* 21. In the UK, the data controller was initially called a data user in the Data Protection Act of 1984.

83 In the Dutch WBP (see ch 5 par 4.3.3).

84 Also see Bygrave *Data protection law* 21.

85 See the Dutch WBP (ch 5 par 4.3.3).

demonstrated,[86] does not provide adequate protection for personal data, various South African legal writers over the years have expressed the view that data protection legislation is required.[87] But it is only since the introduction of the Constitution in 1996[88] that the legislature has shown any urgency about adopting such legislation.[89] The purpose of this study is to provide guidelines for the development of a statutory South African data protection regime.

2.1 Comparative law approach

In order to establish the essential elements of a data protection law for South Africa, a comparative study of data protection laws is undertaken. Comparative law is a valuable discipline which enables one to gain a better understanding of one's own national law and of ways of improving it.[90] The comparative approach is therefore helpful in gaining new knowledge and insights when considering legal reform.[91] A comparative law approach is also essential in any area where harmonisation of international laws is required.[92] Since transborder data flows have resulted in data protection becoming an international issue,[93] it is evident that a comparative approach should be adopted for the harmonisation of data protection laws.[94] Finally, a cross-

86 See ch 7 par 3.

87 See Neethling *Privaatheid* 406; 1980 *THRHR* 141, 155; *Databeskerming* 105 *et seq; Persoonlikheidsreg* 327 *et seq;* Burchell *Personality rights* 398–399; McQuoid-Mason *Privacy* 195 *et seq*; Eiselen *Reg op privaatheid in die inligtingsera* par 7; Roos 1990 *TSAR* 264, 265; Schulze 1994 *THRHR* 75, 85–86.

88 Constitution of the Republic of South Africa Act 108 of 1996.

89 See ch 8 par 4.1.

90 David & Brierley *Major legal systems* 6.

91 Venter et al *Regsnavorsing* 71 208–209.

92 David & Brierley *Major legal systems* 10.

93 See ch 3 par 1.

94 Bygrave *Data protection law* 12 also argues that "as data-processing operations increasingly extend across national boundaries, the way in which they are to be regulated should not occur without consideration of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation". On harmonisation, also see Sieghart (continued...)

national perspective is analytically fruitful given the fact that all countries' data protection laws are based upon and embody a set of broadly similar principles.[95]

The countries elected for this study are the United States, the United Kingdom and the Netherlands. The United States and the United Kingdom represent the common law family, whereas the Netherlands represents the civil law family.[96] This representation is, however, not of any substantial significance since, as was stated previously, all countries' data protection laws are based upon broadly similar principles. But be that as it may, despite the fact that the United Kingdom and the United States represent the same legal family, there are significant differences in the way in which data protection has been approached in these two countries. In the first place, it is noteworthy that while the United States has recognised and protected a right of privacy since early on, to this day the United Kingdom does not recognise a right of privacy under common law.[97] Further, the United States adopted its first piece of data protection law as early as 1974, whereas the United Kingdom dragged its feet on the issue until 1984. The position of the United States is characterised by a piecemeal approach to different areas of data processing and an absence of an effective oversight body, whereas the United Kingdom has a much more unified approach to data processing. It also has an extensive oversight regime. The Netherlands and the United Kingdom represent the modern approach to data protection.[98] The approach of the United States nevertheless requires careful study because of this country's different approach to data protection and its dominant role internationally in the information technology arena.

94(...continued)
"Protection of personal data" 224.

95 Bygrave *Data protection law* 12.

96 The choice of the Netherlands as representative of the civil law family was partly influenced by the fact that the Dutch legal texts were more accessible (from a language point of view) for the writer of this thesis, whereas eg French, German, Norwegian and Swedish texts, all of which would also have been excellent choices, are not. However, the decision to choose the Netherlands turned out to be an inspired one in the light of the excellent data protection regime in that country.

97 Privacy is protected under the Human Rights Act of 1998.

98 There are more similarities between the UK and the Netherlands than there are between the UK and the USA. The statutes of both the Netherlands and the UK were drafted to implement the EU Directive on data protection. See ch 4 par 4.2.2 and ch 5 par 4.2.2.

The international character of data protection obviously also necessitates a study of various documents on data protection drafted by international organisations, such as the Organisation of Economic Co-operation and Development (OECD), the Council of Europe and the European Union. It is essential that any data protection legislation adopted should conform to international standards in this area.[99]

2.2 Private law approach

The study has been undertaken from a private law perspective. The interests involved (privacy and identity)[100] are protected in South African private law as personality interests. However, the right to privacy is also protected as a fundamental human right and the influence of constitutional law on data protection will therefore be considered as well.[101]

2.3 Legal positivistic approach

Since data protection is regulated by means of legislation in all the countries studied, a discussion of the applicable different national statutes makes up a major part of this study. The study therefore also follows a legal positivistic approach in which the different pieces of legislation are analysed in detail and commented on.[102] Problem areas and weak points as well as positive aspects of all the laws are highlighted. This makes it possible to avoid pitfalls when drafting new data protection legislation for South Africa and to ensure that all the essential elements of data protection are incorporated into any new law.

99 See ch 3.

100 See ch 7 par 2.3.2.1.

101 Privacy and identity are also directly or indirectly protected by criminal sanctions such as *crimen iniuria* (see further Snyman *Criminal law* 428–434). Criminal law falls outside the scope of this thesis and will not be discussed.

102 Venter et al *Regsnavorsing* 63–66.

2.4 Outline

The different legal instruments for data protection are discussed in more or less chronological sequence, which makes it possible to trace the developments in the area of data protection over the years.[103] The position in the United States is discussed in chapter 2. The first statutes in the United States that introduced data protection principles,[104] were adopted in 1970[105] and 1974.[106] The international documents concerning data protection are discussed in chapter 3. The first international documents were adopted in 1981.[107] Chapter 4 deals with the position in the United Kingdom, where the first data protection legislation was promulgated in 1984.[108] Chapter 5 discusses the position in the Netherlands where data protection laws date from 1989.[109] In chapter 6 comparative conclusions are drawn from the previous chapters and a number of data protection principles are identified that are reflected in all the laws discussed.

Chapter 7 analyses the private law foundations of the legal protection of the data subject in South African law from a theoretical point of view. The protection of the two interests involved, namely privacy and identity, is discussed with reference to the elements of a delict. General principles of data protection as viewed from a private law perspective are identified. Chapter 8 discusses the extent to which the protection of the data subject has been achieved in South African positive law, either in case

---

103 As Bygrave *Data protection law* 87–88 says:"Moving from the oldest of the data protection instruments to the youngest, we can discern certain regulatory trends. In data protection discourse, it is popular to categorise these trends as in terms of 'generations'; ie, one generates between , ia, 'first-', 'second-', and 'third-generation' data protection laws." See further ch 6 par 2.5.4.

104 Referred to as "fair information principles" in the USA.

105 Fair Credit Reporting Act of 1970.

106 Privacy Act of 1974.

107 Viz the European Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. This was followed by the European Union's Directive on data protection in 1995.

108 Data Protection Act of 1984, replaced by the Data Protection Act of 1998.

109 Wet Persoonsregistraties (WPR) (Registration of Persons Act) of 1989. Replaced by the Wet Bescherming Persoonsgegevens (WBP) (Personal Data Protection Act) of 2000.

law or in legislation. In chapter 9, in conclusion, the essential provisions that should be included in a data protection law are identified.