FEATURES OF THE PROTECTION OF PERSONAL INFORMATION BILL, 2009 AND THE LAW OF DELICT

Thirty-five years ago I came to the conclusion in my doctoral thesis on the right to privacy that the introduction of so-called data-protection legislation in our country was urgently necessary, in order to protect persons (natural or juristic) against the processing of their personal information by the state and private persons (individuals and corporations alike).[1] In my inaugural lecture as professor at the University of South Africa in 1979, I reiterated the need for such legislation (with specific focus on the activities of credit bureaux).[2] In 2002 I was appointed as leader of Project 124 of the South African Law Reform Commission dealing with privacy and data protection with the aim of developing draft legislation for South Africa. The report, including the Protection of Personal Information Bill, was published in February 2009[3] and submitted to the Minister of Justice and Constitutional Development for consideration by the government. After two years there is still no confirmation that the Bill will become law. Against this background I decided to move full circle at my *alma mater*, the University of the Free State, by returning to the topic of my first inaugural lecture.

It stands to reason that the complexities of modern society have produced ever more reasons why the state or persons have an interest in and an ever growing need for information about other persons. In order to obtain these data and satisfy the need, a new industry has developed, the practices of which, especially due to the use of computers, pose an immense potential threat to the personality of persons, primarily to their privacy and identity. In particular, integrated data banks (principally through the internet)[4] create the possibility of the visibility of a person's private life (so-called computer privacy) as never before.[5]

---

1 See Neethling 1976:406; see also Roos 2008:65; Roos 2010:***.
2 See Neethling 1980:141.
3 See SALRC 2009:i-iii.
4 See Roos 2007:401.
5 See Roos 2003:1-14; Roos 2010: ***-***; Neethling *et al* 2005:267. Miller 1972:429 fn 1 puts it succinctly as follows: "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."

In view of the extent and seriousness of the threat to privacy,[6] well over 50 countries have by 2009 introduced data-protection legislation.[7] It is therefore surprising to find that in South Africa, apart from common-law principles and a few statutes, such as the National Credit Act, that deal directly with specific instances of the protection of personal information,[8] no encompassing Act has yet been adopted. This is all the more surprising since the entrenchment of the right to privacy in the Bill of Rights[9] places an obligation on the state to respect, protect, promote and fulfil this fundamental right.[10] Be that as it may, the state did initiate steps in this regard by approaching the Law Reform Commission to thoroughly investigate the matter and this resulted in said report and the proposed Protection of Personal Information Bill.

Before dealing with the Bill, it is for purposes of clarity necessary to have a closer look at the concepts of privacy and identity. Privacy is a human (or corporate)[11] sphere of seclusion from the public, embracing all those personal facts or information which the person concerned has excluded from the knowledge of others[12] and with regard to which he has the will that they be kept private.[13] Examples of such information include facts

---

6 See Neethling *et al* 2005:268-269 as to the current extent of the processing of personal information by private and public data processors.

7 See SALRC 2009:6; see also Roos 2010 ***.

8 Eg the National Credit Act 34 0f 2005; the Electronic Communications and Transactions Act 25 of 2002; the Promotion of Access to Information Act 2 of 2000; see Van der Merwe *et al* 2008:358-367; Roos 2008:94; Roos 2003:660-669, 710-715; Roos 2007:424-433.

9 Constitution s 14.

10 Constitution s 7(2).

11 A juristic person's privacy is probably analogous to that of natural persons (see Neethling *et al* 2005:32 fn 336). There is no indication in the Bill of Rights that the state and its organs as public juristic persons have any fundamental rights (and thus also the personality rights to privacy and identity) at its disposal. On the contrary, the Bill "enshrines the rights of all people in our country" (Constitution s 7(1)), and is therefore only available to natural persons (and where applicable to private juristic persons) who are then protected against *inter alia* arbitrary state actions. Seen thus, it would be contrary to the purport, spirit and objects of the Bill of Rights to develop the common law by recognising that the state also dispose of these rights (cf Constitution s 39(2); Neethling 2011a:*** ff).

12 The constitutional concept of privacy also embraces so-called informational privacy (see Neethling 2010:782 fn 8; see eg *Bernstein v Bester* 1996 2 SA 751 (CC); *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*; *In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 1 SA 545 (CC); *Mistry v Interim Medical and Dental Council of South Africa* 1998 4 SA 1127 (CC); *Pretoria Portland Cement Co Ltd v Competition Commission* 2003 2 SA 385 (SCA):408-409, 411; *Harksen v Lane* 1998 1 SA 300 (CC):331-332; *Klein v Attorney General, WLD* 1995 3 SA 848 (W): 865; *Nel v Le Roux* 1996 3 SA 562 (CC):568-571; see also McQuoid-Mason 2000: 249.

13 See eg *National Media Ltd v Jooste* 1996 3 SA 262 (A):271; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T):384; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T):553; *Huey Extreme Club v McDonald t/a Sport Helicopters* 2005 1 SA 485 (C):494; *Deutschmann*; *Shelton v Commissioner for the SARS* 2000 2 SA 106 (E):123; cf *NM v Smith (Freedom of Expression Institute as amicus curiae)* 2007 5 SA 250 (CC):262; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A):462; *Bernstein v Bester* 1996 2 SA 751 (CC):789; see also Roos 2006:106 fn18; Roos 2007:421-422; Roos 2008:90-91; Roos 2010:***; SALRC 2009:22). The will to keep information private is an important component of privacy: absent a will to keep a fact private, absent an interest in privacy worthy of protection (*National Media Ltd v Jooste* 1996 3 SA 262 (A):271).

about a person's health,[14] family and sex life,[15] financial position and creditworthiness.[16] A person may prevent others from intrusion into his private sphere (for instance by peeping,[17] eavesdropping[18] or shadowing[19]), or from disclosing private facts to third parties where he is entitled to dictate the ambit of the disclosure to a medical doctor or financial adviser, a circle of family or friends or the public at large.[20] Each person himself therefore determines the destiny of his private information and consequently the scope of his interest in privacy. This is a very important aspect of data protection, the aim of which is in essence to enable a person to have effective control over the processing of his personal information (for example, by a credit bureau, a bank, an insurance company, her employer, or the medical profession).[21] On the other hand identity is that uniqueness which identifies each person as a particular individual (or corporation)[22] and as such distinguishes him from others. Identity manifests itself in various characteristics by which a person can be recognised, for example her life history, name, voice, handwriting or physical image. Identity is usually infringed by its misrepresentation, that is, if a characteristic thereof is used in a way that does not reflect the person's true (own) image.[23] [24] A frequent distortion of identity nowadays occurs through identity theft. Since truthfulness is an element of infringement of privacy, while falsity is an element of infringement of identity,[25] privacy is threatened by the processing of true personal

---

14 Eg *Tshabalala-Msimang v Makhanya* 2007-08-30 case no18656/07 (W); *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A); *NM v Smith (Freedom of Expression Institute as amicus curiae)* 2007 5 SA 250 (CC).

15 *Prinsloo v RCP Media Ltd t/a Rapport* 2003 4 SA 456 (T).

16 See Neethling et al 2005:268-269.

17 Eg *MEC for Health, Mpumalanga v M-Net* 2002 6 SA 714 (T):718–719, 721.

18 Eg *S v A* 1971 2 SA 293 (T); cf *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A):463.

19 Eg *Epstein v Epstein* 1906 TH 87; *Huey Extreme Club v McDonald t/a Sport Helicopters* 2005 1 SA 485 (C):498–499.

20 See *National Media Ltd v Jooste* 1996 3 SA 262 (A):271 where Harms JA put it as follows: "The individual concerned is entitled to dictate the ambit of disclosure eg to a circle of friends, a professional adviser or the public. . . He may prescribe the purpose and method of the disclosure. . . Similarly, I am of the view that a person is entitled to decide when and under what conditions private facts may be made public." See also Neethling *et al* 2005:31; Neethling 2005:19-20; Roos 2007:421-422; Roos 2010:***.

21 See Neethling et al 2005:268-209.

22 Just like a juristic person's privacy (supra fn 11), its identity is also analogous to that of natural persons (see Neethling 2011:64).

23 *Grűtter v Lombard* 2007 4 SA 89 (SCA):93 95-96, with reference to Neethling *Persoonlikheidsreg* 44–45; see also Neethling *et al* 2005:32; Loubser, Midgley *et al* 2010: 55-66, 325-327; Roos 2008:91-92.

24 Identity may also be infringed where it is misappropriated for commercial purposes. These instances may also qualify as a falsification or misrepresentation of identity (see Neethling *et al* 2005:37 256 fn 12). But, as Cornelius 2008:662-664 persuasively argues, falsification should not be a necessary requirement. The mere use of *indicia* of identity for commercial purposes should in principle infringe a person's identity.

25 See Neethling 2005:24.

information, whereas identity is endangered by the processing of false or misleading data.[26]

An important basic question for the Law Reform Commission was whether legislative data-protection measures should be adopted to counter the threat to the rights to privacy and identity; or whether it should be left to the courts to utilise traditional principles of the law of delict directed at the protection of these personality rights in our law,[27] and to develop and adapt them for the protection of personal information. However, in view of the inherent conservatism of the courts, it is improbable - even if they fully comply with their general obligation to develop the common law in the light of the values underpinning the Bill of Rights[28] - that the application of the traditional principles in case law will occur often or extensively enough in the near future. Moreover, since the major engine for law reform should be the legislature and not the judiciary, and the introduction of a data protection regime will not merely involve incremental changes of the common law but radical law reform, it is a task for the legislature.[29] This is all the more true since effective data protection requires that, apart from the traditional principles, persons themselves (the data subjects) should also be able to exercise a measure of active control over their personal data. In fact, the traditional measures have little value if such active control over the processing of personal data is absent. As will be demonstrated, the active control principles differ completely from traditional privacy protection in terms of the law of delict and therefore are unique in this field. Consequently such measures can be created by legislation only.[30] Finally, many countries, especially in Europe, will require adequate data protection in South Africa, which the common law does not provide, for the continued free cross-border flow of personal information.[31] The Commission therefore recommends

---

[26] See Roos 2003:545 554 ff; Roos 2007:422; Neethling *et al* 2005:270-271.

[27] See SALRC 2009:14-42; Roos 2003:543-544; Neethling 2005:272-278.

[28] See Constitution s 39(2); *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)* 2001 4 SA 938 (CC):953 ff; see also *Van Eeden v Minister of Safety and Security (Women's Legal Centre Trust*, *as amicus curiae)*2003 1 SA 389 (SCA):395; *Minister of Safety and Security v Van Duivenboden* 2002 6 SA 431 (SCA):444; *Dendy v University of the Witwatersrand, Johannesburg* 2005 5 SA 357 (W):371–372; Neethling & Potgieter 2010:17; Roos 2003:548 649-650.

[29] *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)* 2001 4 SA 938 (CC):955; Neethling *et al* 2005:272; SALRC 2009:42.

[30] See Roos 2003:644-649; Roos 2007:423; Roos 2008:92; Neethling *et al* 2005:278-280.

[31] See Roos 2003:477-479; Neethling *et al* 2005:281.

the introduction of legislative data-protective measures as reflected in the Protection of Personal Information Bill.

The main features of the Bill, which according to Roos[32] complies in all important aspects with international standards, can be summarised as follows:

(a) Personal information protection will be regulated by a general, omnibus statute applicable to both the state[33] and the private sector. Automatic and manual processing will be covered and identifiable natural and juristic persons[34] will be protected. Exempted from the Bill are *inter alia* the processing of personal information by the Cabinet and the courts, and for purposes of purely personal or household activities, national security or defence, criminal investigation and prosecution, and journalism.[35]

(b) General principles of protection will be applicable to the processing of personal information. There is general agreement on the eight core data-protection principles which should be embodied in any effective data-protection regime, and numerous countries have adopted them in their data-protection legislation.[36] They are accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data-subject participation. These principles will be discussed in more detail later.[37] Special provision has furthermore been made for the protection of so-called sensitive personal information relating to children, religion or philosophy of life, race, trade- union membership, political persuasion, health and sexual life, and criminal behavior.[38] It stands to reason that allowance had to be made for exceptions to or exemptions from the application of the data-protection

---

[32] See Van der Merwe *et al* 2008:389.

[33] The principle of legality, which is recognised in both the Constitution and at common law, and in terms of which state officials have no authority nor may they excercise any function apart from those expressly granted to them by law, will be applicable to the processing of personal information by the state. Such infringement of privacy or identity by state officials may therefore only be justified if they had the authority to do so (cf as to violation of liberty by state officials *Tobani v Minister of Correctional Services* [2002] 2 All SA 318 (SEC):326-327; *Minister of Correctional Services v Tobani* 2003 5 SA 126 (E):133-137; *Sex Worker Education and Advocacy Task Force (SWEAT) v Minister of Safety and Security* 2009 6 SA 513 (WCC):523).

[34] See also Neethling 2008:500ff.

[35] See SALRC 2009:37-103; cl 3-6 of the Bill.

[36] Cf Roos 2006:107 ff; Roos 2003:480 ff.

[37] See SALRC 2009:105-202; cl 7-24 of the Bill.

[38] See SALRC 2009:202-224; cl 25-32 of the Bill.

principles. Such exemptions and exceptions are for example granted to data processors where the risk to the privacy of the relevant person or persons is relatively small, or where other private interests or the public interest override the right to privacy.[39]

(c) Since it would be impossible for a person to ensure that the data-protection principles are adhered to by the data industry, provision has been made for the creation of an independent data protection regulatory authority, headed by a Regulator, to supervise the activities of the data industry.[40] The Regulator will, *inter alia*, be responsible for the implementation of the Bill. Data processors will be under an obligation to notify the Regulator of any processing of personal information before they undertake such processing. The Regulator must enforce the Bill, using as a first step a system of notices where conciliation or mediation has not been successful. Failure to comply with the notices will be a criminal offence. The Regulator may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered.

(d) A flexible approach would be followed in which data-processing industries may develop their own codes of conduct (in accordance with the data-protection principles set out in the Bill) which will be overseen by the regulatory agency.[41]

(e) Specific provision has been made for the protection of data subjects' rights in so far as direct marketing in the form of unsolicited electronic communications (spam) and automated decision making are concerned.[42]

(f) Finally, the Law Reform Commission has strived for an adequate level of personal information protection in the Bill in terms of the relevant European Union Directive.[43] In

---

[39] See SALRC 2009:225-230; cl 33-34 of the Bill.
[40] See SALRC 2009:299-378; cl 35-56 of the Bill.
[41] See SALRC 2009:379-392; cl 57-65 of the Bill.
[42] See SALRC 2009:232-275; cl 66-68 of the Bill.
[43] See Roos 2007:406-416 for a brief overview of its provisions.

accordance with the Directive the Bill prohibits the transfer of personal information to countries that do not ensure an adequate level of protection.[44]

We now return to the eight core data-protection principles with the aim of demonstrating to what extent each of them is in accordance with or supplementary to the common law principles of the law of delict as informed by the Bill of Rights.

Principle 1: Accountability.[45] The party responsible for the processing must ensure that the information-protection principles are complied with. The responsible party will be accountable for any interference with the protection of the personal information of a data subject and liable for any breach of the principles.[46] This principle is really self-evident and in line with the common law position that the person processing personal data can be prohibitorily or mandatorily interdicted, or will be liable - and thus accountable - for the wrongful infringement of privacy or identity.[47] However, whereas intent or negligence is a requirement for liability at common law, according to the Bill liability is strict. Furthermore, in terms of the law of delict, private data processors can be directly as well as vicariously liable, while the state can only be vicariously liable.[48] But since the Bill does not make any distinction between the state and private responsible parties, it seems that the state can also be directly liable for breach of the protection principles. Finally, an obvious fundamental difference between the law of delict and the Bill is that the Regulator ensures that responsible parties adhere to the data-protection principles, while at common law the data subjects themselves must enforce protection of their privacy and identity against the activities of the data industry.

---

[44] See SALRC 2009:277-297; cl 69 of the Bill.

[45] See SALRC 2009:121-123; Van der Merwe *et al* 2008:379-380; cl 7 of the Bill.

[46] See cl 70 ff of the Bill as to enforcement by the Regulator and cl 94 of the Bill as to an action for damages. As to the latter, provision is made for patrimonial and non-patrimonial damages, as well as aggravated damages. The latter should not be equated with punitive damages (cf Neethling 2008b:173 ff).

[47] See Neethling *et al* 2005:278.

[48] S 1 of the State Liability Act 20 of 1957 provides that the state is liable for "any wrong committed by any servant of the State acting in his capacity and within the scope of his authority as such a servant". Seen thus, the state can only be vicariously liable for the delicts of its employees (cf Loubser, Midgley *et al* 2010: 257-258; Neethling & Potgieter 2010:368; *Masuku v Mdlalose* 1998 1 SA 1 (A):14-16; *Mhlongo v Minister of Police* 1978 2 SA 551 (A):567). The contrary opinion expressed in *Minister of Safety and Security v F* 2011 3 SA 487 (SCA):499-500 504 is therefore questionable. This conclusion does not mean that private employers are also excluded from direct liability (see eg *Media 24 Ltd v Grobler* 2005 6 SA 328 (SCA) 349 ff). See generally Neethling 2011b:***-***.

Principle 2: Processing Limitation.[49] This principle embraces four aspects limiting the processing of personal information to ensure that the processing is done by lawful means.[50]

First of all, it is emphasised that the processing of personal information must be done lawfully and in a reasonable manner in order not to infringe the privacy of the data subject. This means that the processing must not only comply with the provisions of the Bill but also with other relevant law.[51] If so, the processing will be lawful and by implication not an unreasonable infringement of privacy. Seen thus, the addition of the reasonableness criterion seems to be superfluous.[52] It stands to reason that this principle is also part of common law. To be lawful, the processing of personal information must be reasonable in terms of the test for delictual wrongfulness.[53] As a starting point it must be accepted that the unauthorised processing of personal information is in principle (in the absence of justification) unreasonable and thus *prima facie* wrongful. Generally speaking no person has to tolerate information concerning him being processed.[54] If such an infringement of privacy or identity is found to be unreasonable, the processing will be wrongful.[55]

The second qualification limiting processing, namely that of minimality, provides that personal information may only be processed if, given the purpose(s) for which it is processed, it is adequate, relevant, and not excessive.[56] This requirement fits comfortably with the third limitation qualification, that is justification, since especially

---

[49] See SALRC 2009:123-138; Van der Merwe *et al* 2008:372-373; cl 8-11 of the Bill.

[50] See Van der Merwe *et al* 2008:372

[51] The processing of personal information which has been acquired by a wrongful act of intrusion into privacy, such as illegal wiretapping or concealed video cameras, will in principle not be lawful (see eg *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A):463; *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 3 SA 56 (W):61; *MEC for Health, Mpumalanga v M-N et* 2002 6 SA 714 (T)).

[52] Cf Roos 2003:483.

[53] See as to this test, Neethling & Potgieter 2010:33ff; Roos 2003:574-588; SALRC 2009:28-29; Neethling *et al* 2005:221-222, 255-256, 274; Neethling 2011:67. The recent formulation of one variation of the test for wrongfulness in our law, namely that wrongfulness depends on whether it would be reasonable to hold the defendant liable (see eg *Le Roux v Dey* 2011 3 SA 274 (CC):315; *Hawekwa Youth Camp v Byrne* 2010 6 SA 83 (SCA):90-91), is controversial, subject to criticism and therefore not acceptable (see Neethling & Potgieter 2010:78-82).

[54] See Roos 2003:581; Roos 2006:108; Van der Merwe *et al* 2008:356; Neethling *et al* 2005:274; SALRC 2009:29-30.

[55] The bounds of reasonableness will eg be exceeded if data which have been obtained in an unlawful manner (such as by shadowing a person: see *Huey Extreme Club v McDonald t/a Sport Helicopters* 2005 1 SA 485 (C):498–499), are processed; see also *supra* fn 39).

[56] See Van der Merwe *et al* 2008:372; cl 9 of the Bill.

relevancy and necessity are indicative of the boundaries of justification. If information is not connected with or unnecessary for the purpose of the processing, it will be unlawful.[57] The requirement of adequacy on the other hand seems to be more concerned with the quality of the information since inadequate information, although true, may create a misleading or inaccurate impression of the data subject.[58] If so, the processing will be unlawful.[59] The qualification of minimality is by implication also implemented at common law. Relevancy is, for example, a requisite for privilege as a ground of justification in instances of infringement of privacy and identity;[60] processed data must be reasonably necessary for the protection of the data processor's legitimate interests,[61] and the misrepresentation of a person's identity by processing inadequate information cannot be justified.[62]

Thirdly, processing is limited by the fact that personal information may only be processed if the data subject has consented to the processing, or if the processing is justified by another ground of justification relating to the protection of the public interest or the legitimate interests of the data subject, the data processor or a third party.[63] In the same vein the law of delict recognises that data processing may be justified by consent, and the legitimate interests of persons or the public interest.[64] [65]

The final qualification limiting processing is that, as a rule, personal information must be collected directly from the data subject.[66] This requirement overlaps with the principle of openness which provides that the data subjects should be aware of the fact that

---

57 See Van der Merwe *et al* 2008:372.

58 Cf Neethling 2008:284 fn 193. Seen thus, the adequacy requirement overlaps with principle 5 on information quality, which obliges the responsible party to ensure, *inter alia,* that the information is not misleading (see *infra* for a discussion). Roos (see Van der Merwe *et al* 2008:372) seems to regard the concepts "adequacy" and "not excessive" in cl 9 of the Bill as synonyms where she remarked that both indicate "that the processing of unnecessary information could render data processing wrongful". Surely the two concepts were meant to have different meanings.

59 It stands to reason that the processing of misleading information will be wrongful.

60 Cf eg *Herselman v Botha* 1994 1 SA 28 (A):35–36; *Naylor v Jansen; Jansen v Naylor* 2006 3 SA 546 (SCA):554; *NEHAWU v Tsatsi* 2006 6 SA 327 (SCA):332; Neethling & Potgieter 2010:337 as to defamation; Neethling *et al* 2005:251-252, 261 as to infringement of privacy and identity.

61 Cf eg *Gosschalk v Rossouw* 1966 2 SA 476 (C):490-492; Neethling *et al* 2005:244 fn 222, 276.

62 See *Grütter v Lombard* 2007 4 SA 89 (SCA):96; Neethling 2011: 70, 73.

63 See Van der Merwe *et al* 2008:372-373; cl 10(1) of the Bill.

64 See Roos 2003:602ff; Van der Merwe *et al* 2008:356-357; SALRC 2009: 34-40; Neethling *et al* 2005:275-278.

65 In terms of cl 10 (2) a data subject may under certain conditions object to the processing of personal information. If so, the responsible party may no longer process the information (see SALRC 2009:136).

66 See Van der Merwe *et al* 2008:373-374; cl 11(1) of the Bill.

information about them is being collected.[67] As Roos[68] pointed out, one way that the data subject can learn about this is to be approached directly for the information. Naturally provision had to be made in the Bill for exceptions to this requirement.[69] It is for instance not necessary to comply with it if the information is contained in a public record or has been made public by the data subject; or where the information from another source is necessary for, *inter alia*, the purposes of criminal investigation and prosecution, the collection of tax revenue, court proceedings, national security, or to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied. The requirement that personal information must be collected directly from data subjects, enabling them to have knowledge of the processing and thereby providing a basis for their control over the processing, is unknown at common law. This will be discussed in more detail later.

Principle 3: Purpose Specification.[70] This very important principle that personal information must be collected for a specific purpose or purposes underpins every other aspect of the processing of information since it determines the scope of the processing.[71] In terms of the Bill the following three provisions give effect to this principle.

Firstly, personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the party responsible for the processing.[72] Data processing can have a lawful purpose only if the object is to further or protect a legitimate interest, that is an interest recognised and protected by law; and in order that the interest(s) involved may be identified, the purpose must clearly disclose which interests are at stake. For this reason the purpose must be explicitly defined. Without such a definition it will be very difficult to judge whether or not the processing is for a lawful purpose - in other words, whether a legitimate interest is protected.[73] This

---

67 See the discussion *infra* under principle 6.
68 Van der Merwe *et al* 2008:374
69 See cl 11(2) of the Bill; Van der Merwe *et al* 2008:374.
70 See SALRC 2009:138-147; Van der Merwe *et al* 2008:374-375; cl 12-14 of the Bill.
71 See SALRC 2009:146.
72 See Van der Merwe *et al* 2008:374; cl 12 of the Bill.
73 Cf Neethling *et al* 2005: 275.

principle is in conformity with the position at common law where the processing of personal information for the purpose of maintaining, protecting or furthering a legitimate interest is justified and therefore lawful.[74]

Secondly, the responsible party must take reasonable steps to ensure that the data subject is aware of the purpose of the collection of personal information.[75] If data subjects are unaware of it, they can hardly be expected to judge whether the processing that is taking place, is lawful. Consequently this provision provides data subjects with a further basis[76] for controlling the processing of their personal information.[77] This requirement is unknown at common law.

Thirdly, as a rule records of personal information may not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.[78] Where this is the case, the responsible party must destroy or delete the record or de-identify it. This requirement seems to be supplementary to the minimality requirement that personal information may only be processed if, given the purpose for which it is processed, it is not excessive.[79] Provision is made for exceptions to this rule, for example where the data subject has consented to the retention of the record; where it is authorised by law; where the retention is for historical, statistical or research purposes, et cetera.[80] Since obsolete data are generally not necessary for the protection of a legitimate interest and therefore a lawful purpose, retention of such personal information would at common law also be unreasonable and therefore wrongful.[81]

Principle 4: Further Processing Limitation.[82] This principle is in essence an extension of the previous principle of purpose specification. The Bill provides that after collection the

---

[74] See Roos 2003:605-608; SALRC 2009: 35-39; Neethling *et al* 2005: 275.
[75] See Van der Merwe *et al* 2008:375; cl 13 of the Bill. See also cl 17(2) of the Bill, discussed infra under Principle 6.
[76] See also the discussion *supra* under Principle 2.
[77] See Neethling *et al* 2005:278-279.
[78] Van der Merwe *et al* 2008:375; cl 14 of the Bill.
[79] See the discussion *supra* under Principle 2.
[80] See Van der Merwe *et al* 2008:375.
[81] See Roos 2003:607; Neethling *et al* 2005:277; SALRC 2009: 37.
[82] See SALRC 2009:147-159; Van der Merwe *et al* 2008:376; cl 15 of the Bill.

further processing of personal information (use or disclosure) must be compatible with the purpose for which it was collected.[83] As expected, provision is here also made for exceptions, which are, apart from a few additions, similar to the exceptions for the requirement that personal information must be collected directly from the data subject.[84] Among the additions are where the incompatible further processing is necessary to prevent or mitigate a serious and imminent threat to public health or safety, or the life or health of the data subject or another individual; or where the information is used for historical, statistical or research purposes.[85] Since the processing of personal information may under common law only be done for the purpose of protecting a legitimate interest, it follows that the data may be used or communicated only for the protection of such an interest, and that the use of data in a manner incompatible with this purpose will therefore be wrongful.[86]

Principle 5: Information Quality.[87] This principle means that the processed information should be of good quality. For this purpose the responsible party must take reasonably practicable steps, having regard to the purpose for which personal information is collected or further processed, to ensure that the data is complete,[88] not misleading, accurate and updated where necessary. It has already been pointed out that personal information, although true, may create a misleading or inaccurate impression of the data subject.[89] This will probably as a rule be the case where incomplete or outdated personal information is processed.[90] At common law the processing of false or misleading data will also be wrongful since such an infringement of identity cannot be justified.[91]

---

[83] To assess such compatibility, the responsible party must take account of the relationship between the purpose of further processing and the purpose for which the information has been collected; the nature of the information concerned; the consequences of the further processing for the data subject; the manner in which the information has been collected, and any contractual rights and obligations between the parties (cl 15(2) of the Bill).

[84] See the discussion *supra* under Principle 2.

[85] See cl 15(3) of the Bill.

[86] See Roos 2003:606; Neethling *et al* 2005:275-276; SALRC 2009:36.

[87] See SALRC 2009:159-162; Van der Merwe *et al* 2008:376-377; cl 16 of the Bill.

[88] Incomplete information may be misleading.

[89] See the discussion *supra* under Principle 2; see also Van der Merwe *et al* 2008:376-377.

[90] Roos (Van der Merwe *et al* 2008:377) points out that the duty of the responsible party to ensure accuracy is not absolute. If, in spite of taking reasonably practical steps in this regard the information is still inaccurate, the responsible party will not be accountable.

[91] See Neethling *et al* 2005:275; see also the discussion *supra* under Principle 2(ii).

Principle 6: Openness.[92] Responsible parties should comply with the general goals of openness and transparency so that not only the Regulator but also the data subjects know about the processing of their personal information. In this regard the Bill provides that personal information may only be processed after a responsible party has notified the Regulator, and has taken reasonably practicable steps to ensure that the data subject is aware of the following:[93] the fact that the information is being collected;[94] the name and address of the responsible party; the purpose or purposes for which the information is being collected;[95] whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to provide the information; any particular law authorising or requiring the collection of the information; and any further information which is necessary to enable processing in respect of the data subject to be reasonable, such as the recipients or categories of recipients of the information;[96] the nature or categories of the information; and the existence of the right of access to and the right to rectify the information.[97] Of course, provision is here also made for exceptions where the responsible party need not comply with said steps. They are *mutatis mutandis* almost the same as the exceptions for the requirement that personal information must be collected directly from the data subject,[98] but the following have also been added: personal information which is to be used in a form in which the data subject will not be identified or which is used for historical, statistical or research purposes only, or where data subjects have previously been informed about a similar collection for the same purpose(s). It goes without saying that it is of paramount importance that data subjects should have knowledge of the fact that personal information about themselves is being processed by a responsible party. Even the most comprehensive measures for protecting data will be worthless if data subjects are unaware that their privacy or identity is threatened or has actually even been infringed.

---

92 See SALRC 2009:163-169; Van der Merwe *et al* 2008:377; cl 17 of the Bill.

93 In terms of cl 17(3) of the Bill the steps to provide these facts to data subjects must be taken before their personal information is collected if it is collected directly from them (unless they are already aware of those facts). In any other case, the steps must be taken before the personal information is collected or as soon as reasonably practicable after it has been collected.

94 See also the discussion *supra* under Principle 2.

95 See also the discussion *supra* under Principle 3.

96 This will enable the data subject to ascertain whether or not the information was used for the protection of a legally recognised interest (cf Neethling *et al* 2005: 279; Roos 2003:714).

97 The rights of access and rectification will be discussed *infra* under Principle 8.

98 See the discussion *supra* under Principle 2.

As such it provides the foundation for effective control by data subjects over the processing of their personal information.[99] The principle of openness is unknown at common law.

Principle 7: Security Safeguards.[100] This principle implies that personal information should be protected by security safeguards. Poor data security is currently a serious, widespread and high-impact risk to the objective of reducing financial crime.[101] The Bill therefore provides that a responsible party[102] must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures[103] to prevent loss of, or damage to, or unauthorised destruction of personal information; as well as unlawful access to or processing of personal information. Furthermore, a paramount issue raised by the recent series of security breaches, is the duty to notify persons who may be affected by the breach (for example, data subjects accessed for purposes of identity theft).[104] The Bill accordingly provides that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify the Regulator and the data subject(s) in writing as soon as reasonably possible after the discovery of the compromise, but *inter alia* taking into account the legitimate needs of law enforcement. The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including, if known to the responsible party, the identity of the unauthorised person(s) who may have accessed or acquired the personal information. The Regulator may also direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected

---

99 See Neethling *et al* 2005:278-279; Roos 2003:505-510.

100 See SALRC 2009:170-190; Van der Merwe *et al* 2008:378; cl 18-21 of the Bill.

101 See SALRC 2009:187.

102 Or an operator on behalf of a responsible party (see cl 19-20 of the Bill).

103 The measures must identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risk identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards (cl 18(2) of the Bill).

104 See SALRC 2009:188.

by the compromise. As with the principle of openness, the principle of security safeguards is not known at common law.

Principle 8: Data Subject Participation.[105] This principle encompasses that data subjects should be able to participate in, and have a measure of control over, the processing of their personal information. This principle is not recognised at common law. In order to accomplish this, the Bill provides that a data subject has the right to request from a responsible party, firstly a confirmation (free of charge) whether or not the responsible party holds personal information about the data subject; and secondly (at a prescribed fee), a description of the personal information held, including information about the identity of all third parties who have had access to the information.[106] The information must be provided within a reasonable time, in a reasonable manner and format, and in a form that is generally understandable. If information is provided, data subjects must also be informed of their right to request a correction of the information. It stands to reason that this right of access[107] is necessary for effective control of data, for only thus will such person be able to ascertain whether, for example, the information is correct, necessary for the purpose(s) for which the data are being processed, et cetera.[108]

In terms of their right to request a correction of their data, data subjects may ask a responsible party to correct, delete or destroy personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully. The responsible party must then either correct, destroy or delete the information, or provide the data subject with credible evidence supporting the information; or attach to the information an indication that a correction of the information has been requested but has not been made. The responsible party must inform the data subject of the steps taken, and, where reasonably practicable, also inform third parties to whom the personal

---

[105] See SALRC 2009:190-202; Van der Merwe *et al* 2008:379; cl 22-24 of the Bill.

[106] As said (*supra* fn 96), the data subject can then ascertain whether or not the third party had a legitimate interest in the information.

[107] The fundamental right of access to any information held by the state, and to information held by another person which is required for the exercise or protection of a right (Constitution, 1996 s 32), entrenches an individual's right to have access to his personal data record(s). This right is recognised in the Promotion of Access to Information Act 2 of 2000 ss 11 and 50, and the procedure for obtaining access in terms of ss 18 and 53 is applicable to requests for access to personal information made in terms of the Bill (see cl 24). See further Roos 2003:660 ff, esp 672–688; Van der Merwe *et al* 2008:358-360.

[108] See Neethling *et al* 2005:279.

information has been disclosed, of these steps if the changed information affects them. There can be no doubt that the right to correction is essential for preventing or terminating an infringement of the data subject's personality rights to privacy and identity.[109]

From the foregoing it is clear that although the law of delict may be developed by the courts to encompass the data protection principles of accountability, processing limitation, purpose specification, further processing limitation and information quality, the same cannot be said of the principles of openness, security safeguards and data subject participation. For the introduction of these principles legislation will therefore be necessary.

In conclusion, it must again be emphasised that the activities of the data industry create an immense threat to the personality interests of privacy and identity. It is clear that the traditional common law principles protecting these interests are unable to deal effectively with the problems in this field, and that many countries may require adequate data protection in South Africa for the continued free cross-border flow of personal information.[110] Compared to the conclusion reached in my doctoral thesis thirty-five years ago, the adoption of legislation for the protection of personal information is now completely overdue.[111] I therefore appeal to the government to promulgate the Protection of Personal Information Bill of 2009, recommended by the Law Reform Commission, as soon as possible as part of the law of South Africa.[112]

---

[109] See Neethling *et al* 2005:279.

[110] Roos 2008:98 (see also Roos 2007:411-413) expressed it thus: "Despite South Africa's apparently high regard for the individual's right to privacy and identity and our well-developed common and constitutional law of privacy, South Africa does not meet the adequacy requirement of the EU Directive because we do not have a data protection Act. This means that South African participants in the information technology arena are at a constant disadvantage. Contractual clauses have to be used to provide for adequate data protection measures for every international commercial transaction that involves the transfer of personal information from overseas to South Africa, such as the selling of tickets for the World Cup games in the names of specific persons."

[111] Also see Roos 2007:433.

[112] See also Roos 2008:98.

Bibliography

Cornelius S

2008. Die reg op identiteit en die kommersiële ontginning van die individu se openbare beeld. *Journal of South African Law*: 645.

Loubser M, Midgley JR, Mukheiber A, Niesing L & Perumal D

2010. *The Law of Delict in South Africa.* Cape Town Oxford University Press.

McQuoid-Mason DJ

2000. Invasion of privacy: common law v constitutional delict - Does it make a difference? *Acta Juridica*: 227.

Miller AR

1971. *The Assault on Privacy* (*Computers, Data Banks and Dossiers*)

Neethling J

1976. *Die Reg op Privaatheid.* LLD thesis UNISA.

1979. Die kredietburowese en databeskerming. *Tydskrif vir Hedendaagse Romeins-Hollandse Reg*: 141.

2005. The concept of privacy in South African law. *South African Law Journal*: 18.

2008. Data protection and juristic persons. *Tydskrif vir Hedendaagse Romeins-Hollandse Reg*: 500.

2008a. *Van Heerden-Neethling Unlawful Competition*. Durban LexisNexis.

2008b. Die *actio iniuriarum* en bestraffende genoegdoening. *Vita Perit, Labor non Moritur – Liber Memorialis PJ Visser*. Durban LexisNexis: 173.

2010. The right to privacy under South African law. *Festschrift für Helmut Koziol zum 70. Geburtstag.* Vienna Jan Sramek: 781.

2011. ‘n Vergelyking tussen die individuele en korporatiewe reg op identiteit. *Tydskrif vir die Suid-Afrikaanse Reg*: 62.

2011a. Die staat en die reg op pivaatheid. *Tydskrif vir Hedendaagse Romeins-Hollandse Reg*: ***.

2011b. Liability of the state for rape by a policeman: The saga takes a new direction. *Obiter*: ***.

Neethling J & Potgieter JM

2010. *Neethling-Potgieter-Visser Law of Delict*. Durban LexisNexis.

Neethling J, Potgieter JM & Visser PJ

2005. *Neethling’s Law of Personality*. Durban LexisNexis.

Roos A

2003. *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study.* LLD thesis UNISA.

2006. Core principles of data protection law. *CILSA*: 102.

2007. Data protection: Explaining the international backdrop and evaluating the current South African position. *SALJ*: 400.

2008. Personal data protection in New Zealand: Lessons for South Africa? *PER*: 62.

2010. *Privacy in the facebook era: A South African legal perspective*. Inaugural Lecture 2010-10-07 UNISA.

South African Law Reform Commission (SALRC)

2009. Project 127: *Report on privacy and data protection*.

Van der Merwe D, Roos A, Pistorius T & Eiselen S

2008. Data protection. *Information and Communications Technology Law*. Durban LexisNexis.