
PERSONAL DATA PROTECTION IN NEW ZEALAND: LESSONS FOR SOUTH AFRICA?

ISSN 1727-3781



2008 VOLUME 11 NO 4

PERSONAL DATA PROTECTION IN NEW ZEALAND: LESSONS FOR SOUTH AFRICA?

A Roos*

Summary

In 1995 the European Union adopted a Directive on data protection. Article 25 of this Directive compels all EU member countries to adopt data protection legislation and to prevent the transfer of personal data to non-EU member countries (“third countries”) that do not provide an adequate level of data protection. Article 25 results in the Directive having extra-territorial effect and exerting an influence in countries outside the EU. Like South Africa, New Zealand is a “third” country in terms of the EU Directive on data protection. New Zealand recognised the need for data protection and adopted a data protection Act over 15 years ago. The focus of this article is on the data protection provisions in New Zealand law with a view to establishing whether South Africa can learn any lessons from them. In general, it can be said that although New Zealand law does not expressly recognise a right to privacy, it has a data protection regime that functions well and that goes a long way to providing adequate data protection as required by the EU Directive on data protection. Nevertheless, the EU has not made a finding to that effect as yet. The New Zealand data protection act requires a couple of amendments before New Zealand might be adjudged ‘adequate’. South Africa’s protection of the right to privacy and identity is better developed and more extensive than that of New Zealand. Privacy is recognised and protected in the law of delict and by the South African Constitution. 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. It is argued that South Africa should follow New Zealand’s example

* BLC (UP), LLB (Unisa), LLM (Michigan), LLD (Unisa). Associate Professor, Department of Private Law, University of South Africa.

and adopt a data protection law as soon as possible.

PERSONAL DATA PROTECTION IN NEW ZEALAND: LESSONS FOR SOUTH AFRICA?

A Roos*

1 Introduction

1.1 Importance of data protection internationally

Laws that regulate the processing¹ of personal information/data,² referred to as data protection laws,³ have been adopted worldwide since the mid-1970s.⁴ For the European Union⁵ (EU), data protection is such an important issue that it is listed as a fundamental right in the Charter of Fundamental Rights.⁶

* BLC (UP), LLB (Unisa), LLM (Michigan), LLD (Unisa). Associate Professor, Department of Private Law, University of South Africa.

1 Processing refers to any operation which is performed on data. This includes actions such as collection, recording, organisation, storage, adaptation or alteration, retrieval, use, consultation, disclosure, alignment or combination, blocking, erasure, destruction and transmittal.

2 The phrase 'personal information' is used in the sense of information that can be connected to a person. It is usually defined as information relating to and permitting identification of individuals or persons (Bygrave *Data Protection Law 2*). It has been pointed out on another occasion (Roos 2007 *SALJ* 401, n 4) that the two concepts, data and information, are not synonymous (data are unstructured facts or raw material that needs to be processed and organised to produce information) but that in most legal contexts it is unnecessarily pedantic to maintain a distinction between the two concepts (also see Bygrave *Data Protection Law 20*).

3 Sometimes also referred to as privacy laws – see, eg, the USA *Privacy Act* of 1974.

4 The first data protection law was adopted in 1970 in the German state of Hesse. Sweden enacted the first national data protection law in 1973, followed by the USA in 1974. Since then numerous other countries have adopted data protection laws and many have already revised their first data protection laws or have adopted completely new, second-generation laws: the Netherlands adopted its second-generation data protection law in 2000 (*Wet Bescherming Persoonsgegevens 2000*) and the UK adopted its in 1998 (*Data Protection Act* of 1998). On 'generations' in data protection laws, see Bygrave, *supra* n 2, 87-88.

5 The EU flowed from the European Community (EC). The aim of the EC is the attainment of a 'single market' in Europe by removing physical, technical and fiscal barriers. The *Treaty on European Union* (signed in Maastricht in 1992) added political cooperation to the existing Community structure. Since 1993 the EC has also been referred to as the EU, a term that refers to the aim of political union. The EU at present consists of 27 European countries. See also EU 2008 http://europa.eu/abc/index_en.htm 24 Nov.

6 The Charter of Fundamental Rights of the European Union [2000] *Official Journal C* 364/1 62/184

Furthermore, the 1995 Directive on data protection⁷ compels all EU member countries to adopt data protection legislation and to prevent the transfer of personal data to non-EU member countries ('third countries') that do not provide an adequate level of data protection. Adequacy is assessed in the light of all the circumstances surrounding a data transfer operation and consideration must be given to the nature of the data, the country of origin, the country of final destination, and the laws in that country.⁸ Transfers of personal data must be authorised by a member state, notwithstanding the absence of adequate protection in the recipient state, in a number of specific instances where there is a legal basis for the transfer, such as the unambiguous consent of the data subject.⁹ In addition, transfers may also be authorised where the controller adduces 'adequate safeguards' with respect to the protection of privacy, in particular by concluding an appropriate contract with the party receiving the personal information.¹⁰ These provisions result in the Directive

provides the following in art 8: Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
 3. Compliance with these rules shall be subject to control by an independent authority.
- 7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 *Official Journal L 281/31* (hereinafter referred to as "the data protection Directive" and quoted as Dir 95/46/EC). Reference will be made to the 1995 Directive as the "EU Directive on data protection", since it operates among member states of the EU. However, the Directive is actually a European Community (EC) Directive, since it was proposed as a means towards an economic end (Korff *Data Protection Laws in the EU* 8).
- 8 Art 25 Dir 95/46/EC.
- 9 Art 26(1) Dir 95/46/EC. Other acceptable grounds for international transfers listed in art 26(1) are as follows: the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; the transfer is necessary in order to protect the vital interests of the data subject; or the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation, either by the public in general, or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
- 10 Art 26(2) Dir 95/46/EC.

having extra-territorial effect and exerting an influence in countries outside the EU.

Although the USA as a general rule is reluctant to regulate the information industry, it nevertheless concluded an agreement (the 'Safe Harbor' agreement)¹¹ with the EU to ensure that the free flow of personal information between Europe and the USA was not restricted on the EU side due to inadequate personal data protection in the USA.¹² Many other countries outside the EU fold also adopted data protection laws, because of the influence of the Organisation for Co-operation and Development (OECD) guidelines on data protection,¹³ or the influence of the Council of Europe negotiations with the EU to declare that their data protection regimes provide 'adequate' data protection.

11 The 'Safe Harbor' agreement was concluded in 1998 between the US Department of Commerce and the Internal Market Directorate of the European Commission. Organisations in the USA may decide to participate by complying with the 'Safe Harbor' requirements and by declaring publicly that they do so. Their names are added to a list maintained by the US Department of Commerce. Organisations in the EU who want to export personal data to them can consult this list to determine whether particular companies in the USA are participating. See Department of Commerce *Safe Harbor Agreement* <http://www.export.gov/safeharbor> 24 Nov.

12 At federal level, the USA does not have a general data protection law. Instead, different pieces of legislation are involved. Examples are the *Fair Credit Reporting Act* of 1970, the *Privacy Act* of 1974, the *Right to Financial Privacy Act* of 1978, the *Privacy Protection Act* of 1980, the *Computer Matching and Privacy Protection Act* of 1988, the *Electronic Communications Privacy Act* of 1986, the *Telecommunications Act* of 1996 and the *Children's Online Privacy Protection Act* of 1998. This means that different types of personal information are given different levels of protection. The USA is a member of the OECD and several hundred US companies have adopted the OECD *Guidelines* on data protection (see n 13 more detail). In the private sector one finds therefore that fair information practices have been created through industry self-regulation. However, the application of these principles is voluntary and they are not legally binding on the companies. As such they may be changed at any time by the companies involved. The lack of an independent data protection authority is also seen by privacy commentators as a serious flaw in US law (Flaherty *Surveillance Societies* 367).

13 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* Paris, 23 September 1981 (hereafter OECD *Guidelines*). The OECD is an international organisation with headquarters in Paris. It is composed of 30 of the leading industrial states (including *inter alia* all EU member states, Australia, Japan, Korea, Mexico, New Zealand, Norway, Turkey and the USA) sharing the principles of democracy, market economy and respect for human rights (see OECD 2008 <http://www.oecd.org> 24 Nov). The OECD also involves non-member countries in its work. The OECD's affiliation with 70 non-member countries, of which South Africa is one, gives it global reach. See also Kuner *European Data Privacy Law* 36 and par 2.5.1 below.

A finding by the EU¹⁴ that a third country provides adequate data protection results in such a country's being put on a 'white list', and EU member countries may then not impede the transfer of personal data to that country.¹⁵

Despite the apparent importance of data protection, South Africa is lagging behind in this area. For the last three decades South African academics have been pointing out that it is important for South Africa to adopt a data protection Act.¹⁶ Proposals for the adoption of an Act for the protection of personal information have been on the table for more than three years,¹⁷ but it seems as if the political will to enact such an act is absent.

1.2 *Aim of the article*

One may ask whether or not other countries, apart from Europe and, to a certain extent the USA, take data protection seriously. In this regard it is instructive to consider the position in New Zealand. The focus of this article is on the data protection provisions in New Zealand law, with a view to establishing if South Africa can learn any lessons from them.

Before discussing the specific data protection Act (the *Privacy Act* of 1993), the legal background against which this Act operates will be briefly explored. Data protection is an aspect of the right to privacy.¹⁸ It therefore has to be established whether New Zealand law recognises and protects a right to privacy in common law, constitutional law or statutory law. Traditionally, privacy is defined "as the right to be let alone". This definition was made famous in

14 The Commission of the EU (executive branch of the EU) is authorised to negotiate with third countries that fall short on the adequacy provision (art 25(5) Dir 95/46/EC).

15 Art 25(6) Dir 95/46/EC.

16 Neethling argued in favour of data protection legislation in his thesis in 1976 – see *Privaatheid* 406. See also Neethling 1980 *THRHR* 155; *id* "Databeskerming" 105 *et seq*; McQuoid-Mason *Privacy* 195 *et seq*; Eiselen *Reg op privaatheid in die inligtingsera* par 7; Roos 1990 *TSAR* 265; Schulze 1994 *THRHR* 85-86; Burns *Communications Law* 201.

17 See SALRC *Privacy and Data Protection* Discussion Paper 109 <http://www.doj.gov.za/salrc/> 24 Nov.

18 See Bennett *Regulating Privacy* 23; Flaherty, *supra* n 12, xiii; Bygrave, *supra* n 2, 125 *et seq*.

1890 by two American lawyers, Samuel Warren and Louis Brandeis.¹⁹ 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”.²⁰ This claim to self-determination is the essence of a person’s interest in privacy. Today these two basic ideas of privacy, the right to be let alone and the right to control personal information, form the core of data protection, according to Blume.²¹ It stands to reason that without control over one’s personal information, one’s privacy will be greatly diminished and may ultimately be lost.

After the discussion of the legal protection of privacy in New Zealand, the New Zealand data protection Act itself will be considered. Finally, an attempt will be made to draw conclusions from which South Africa can learn some lessons.

2 Data protection in New Zealand

2.1 Introduction

Like South Africa, New Zealand is a 'third' country in terms of the EU Directive on data protection. What this means is that member countries of the EU may export personal data to New Zealand only if New Zealand provides adequate data protection.

Historically New Zealand has strong political ties with the UK. It also has strong trading ties with Europe. New Zealand is a nation of traders and as such depends on the free flow of information to and from it. International trade is always accompanied by the exchange of information and more often than not

19 Warren and Brandeis 1890 *Harv L Rev* 193.

20 Westin *Privacy and Freedom* 7.

21 Blume 1997 *Int R L Computers & Tech* 195. Also see Bygrave 2001 *UNSWLJ* 279-281.

this information can be classified as personal information.²² New Zealand recognised the need for data protection and adopted a data protection Act over 15 years ago. In the words of the New Zealand Law Commission,²³ “the issue in the area of data protection is not whether it is necessary but rather how it should be carried out as efficiently and effectively as possible”.

2.2 The right to privacy in common law

New Zealand received the whole body of English law as it existed in 1840. It therefore also received the English common law.²⁴ The English common law does not recognise a general right to privacy.²⁵ In New Zealand, nevertheless, privacy was always recognised as a 'silent value' in the law, present in certain situations but unexpressed.²⁶ It has been recognised over a long period as a value worth protecting, even if that protection has not expressly been articulated.²⁷ The courts have acknowledged that privacy values underlie and inform other rules of law and infringements of privacy have therefore sometimes been redressed under other heads of common law. For example, the privacy of the home has been protected by torts such as trespass and nuisance; the privacy of the body by criminal offences and torts such as assault, battery, intentional infliction of nervous shock and negligence; the privacy of personal information by breach of contract and torts such as breach of confidence, negligence, copyright, defamation, malicious falsehood and the

22 Consider a transaction such as the selling of an international flight ticket. This kind of transaction involves the transfer of the name and passport number of the individual. The importance of the free flow of information for commerce is expressed by Lloyd *Information Technology Law* 236 in the following terms: "Whilst there may be concerns at the implications of transfers, however, transborder data flows are essential for commercial activities. Many thousands of messages must be transmitted prior to an aircraft flying from London to New York. This will include passenger details. In this context, transborder data flows constitute no mere esoteric topic. If the data cannot flow, planes cannot fly."

23 New Zealand Law Commission Study Paper 19 par 3.53 (hereafter NZLC SP 19).

24 See Greville 2002 LLRX <http://www.llrx.com/> 16 Jun.

25 Rogers *Torts* 464.

26 NZLC SP 19 par 4.1.

27 Burrows "Invasion of Privacy" 745.

tort of passing off, depending on the circumstances.²⁸ Tobin,²⁹ however, points out that these actions do not provide a remedy for every invasion of privacy.

According to Palmer,³⁰ privacy as a legal issue arrived in New Zealand “by osmosis” from overseas. A privacy tort has been developed in the USA since the end of the 19th century.³¹ By the 1960s, four separate privacy torts had been identified by Prosser,³² namely (a) intrusion into the plaintiff’s solitude, seclusion or private affairs, (b) public disclosure of embarrassing private facts about the plaintiff, (c) publicity that places the plaintiff in a false light and (d) appropriation of the plaintiff’s name or image.³³

Growing attention to privacy in New Zealand during the 1970s, evident from the judgments of the courts³⁴ and Acts of Parliament,³⁵ eventually raised the question as to whether or not New Zealand courts³⁶ should follow the lead of

28 NZLC SP 19 par 4.11; Tobin 2000 NZLJ 216.

29 Tobin 2000 NZLJ 216.

30 Palmer 1975 NZLJ 747.

31 Before 1890 no English or US court recognised a right to privacy. Warren and Brandeis, *supra* n 19, wrote their now very famous law review article in that year. In the article they contended that common law implicitly recognised the right to privacy in that the courts had in the past granted relief for the invasion of privacy on a combination of different common law doctrines. Their article “initiated and theoretically outlined a new field of jurisprudence” (see Larremore 1912 *Columbia L Rev* 708).

32 Prosser 1960 *Cal L Rev* 383-389.

33 Prosser’s framework of four torts became widely accepted in the USA and in 1977 the ALI *Restatement (Second) of Torts* accepted this division. But see Bloustein 1964 *NYULR* 962, who criticised the division of the tort of privacy invasion into four separate torts, because it undermined Warren and Brandeis’s axiom of ‘inviolable personality’ and undermined the moral basis of privacy as an aspect of human dignity.

34 From the mid-1970s the NZ courts began to take into consideration the fact that privacy was invaded when assessing damages in other causes of action (*Ramsay v Cooke* [1984] 2 NZLR 680 687 (HC); NZLC SP 9 par 4.61). Privacy as a value was also recognised by NZ courts when applying legislation involving search or interception warrants and police powers (*Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728 737 (CA); *Transport Ministry v Payn* [1977] NZLR 50 64 (CA); *Moulton v Police* [1980] 1 NZLR 443 (CA); see also *Savelio v R* [2005] NZCA 198.

35 Eg, the *Broadcasting Act* of 1976, the *Human Rights Act* of 1977 and the *Crimes Act* of 1961. See further par 2.3 below.

36 The question was also asked in other common law countries. English courts refused to follow the American courts and several judges made strong statements to the effect that English law recognises no right to privacy (see *R v Brown* [1996] AC 543 557 (HL); *R (on the application of Wainwright) v Richmond upon Thames London Borough Council* [2001] EWCA Civ 2062, CA; *Kaye v Robertson* [1991] FSR 62 70; *Malone v Metropolitan Police Commissioner (No 2)* [1979] 2 All ER 620). English courts have, nevertheless, extended

US courts. By 1986 it had been held by a New Zealand high court that New Zealand law recognised a tort of publication of private facts³⁷ (the second of Prosser's four torts). That view gathered momentum³⁸ and was confirmed in 2004 by the New Zealand Court of Appeal in *Hosking v Runting*,³⁹ with a majority of three to two.⁴⁰

In this case, a magazine commissioned a photographer to take pictures of the twin babies of a well-known television presenter. The pictures were taken while the mother was on a shopping trip with the babies. Although the court recognised the existence of a tort of publication of private facts, the application for an injunction was denied because the photographs were taken in a public place.

Gault P summarised the broad content of the tort of invasion of privacy by publication of private facts in the following terms:⁴¹

It is actionable as a tort to publish information or material in respect of which the plaintiff has a reasonable expectation of privacy, unless that information or material constitutes a matter of legitimate public concern justifying publication in the public interest. Whether the plaintiff has a reasonable expectation of privacy depends largely on whether publication of the information or material about the plaintiff's private life would in the particular circumstances cause substantial offence to a reasonable person. Whether there is sufficient public concern about the information or material to justify the publication will depend on whether in the circumstances those to whom the

the boundaries of the remedy of breach of confidence (influenced also by the *Human Rights Act* of 1998) to such an extent that by 2004 the House of Lords had awarded damages to celebrity model Naomi Campbell when a newspaper published details of drug therapy she was undergoing, together with a photo of her outside a rehabilitation centre (*Campbell v MGN* [2004] 2 AC 457 (HL)). See also *Douglas v Hello!* [2001] QB 967; [2001] 2 All ER 289.

37 See *Tucker v News Media Ownership* [1986] 2 NZLR 716 (HC) discussed by Tobin, *supra* n 29, 217.

38 See *Bradley v Wingnut Films* [1993] 1 NZLR 415; *P v D* [2000] 2 NZLR 591; *L v G* [2002] DCR 234, [2002] NZAR 495. Also see Tobin 2004 *TLJ* 95 96-99 for a short overview of the early development of privacy interests in New Zealand.

39 *Hosking v Runting* [2005] 1 NZLR 1 (CA).

40 See NZLC SP 19 par 4.73. See also *Rogers v Television New Zealand* [2007] NZSC 91; *Andrews v TVNZ* [15 December 2006] HC AK CIV 2004-4-4-353.

41 *Hosking v Runting* [2005] 1 NZLR 1 32 (CA).

publication is made can reasonably be said to have a right to be informed about it.

In essence, two elements have to be proved: the existence of facts in respect of which there is a reasonable expectation of privacy; and publicity given to those private facts that would be considered highly offensive⁴² to an objective, reasonable person.⁴³

Publication could be justified by the fact that the information involves a legitimate public concern.⁴⁴ The court emphasised that “the scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society”.⁴⁵ The court was of the opinion that the defence of legitimate public concern will ensure this. The court held that the “significant value to be accorded freedom of expression requires that the tort of privacy [infringement] must necessarily be tightly confined”.⁴⁶ The competing values of the privacy of the individual and the public’s right to receive information have to be balanced. Before publication will be allowed, the level of public concern must outweigh the level of harm likely to be caused by the publication.⁴⁷ The primary remedy upon a successful claim is an award of damages, but injunctive relief may be appropriate in some circumstances.⁴⁸

As far as the tort of intentional intrusion is concerned (the third of Prosser’s torts), this has received less consideration by the New Zealand courts and Tobin argues that it “is perhaps still arguable whether it exists in New Zealand”.⁴⁹ The court in *Hosking* expressly did not answer the question

42 One of the majority judges, Tipping J, would settle for 'substantially' offensive publication – *ibid* 61-62.

43 *Hosking v Runtig* [2005] 1 NZLR 1 32 (CA).

44 *Ibid* 32.

45 *Ibid* 35.

46 *Ibid* 35-36.

47 *Ibid* 36. The fact that minor children are involved, as in *Hosking*, should be taken into account. The court emphasised that “the vulnerability of children must be accorded real weight and their private lives will seldom be of concern to the public” (at 38).

48 *Ibid* 38.

49 Tobin, *supra* n 29, 217. See *TV3 Network Services v Farhey* [1999] 2 NZLR 129 which

whether intrusion into seclusion or solitude will be included under the tort of invasion of privacy:⁵⁰

... we emphasise that at this point we are concerned only with the third formulation of the privacy tort identified by Prosser and developed in the United States cases: wrongful publicity given to private lives. We need not decide at this time whether a tortious remedy should be available in New Zealand law for unreasonable intrusion into a person's solitude or seclusion ...

The fourth of Prosser's torts, namely "appropriation of plaintiff's name or image", was expressly rejected in the *Hosking* case; the court held that there was no cause of action in New Zealand law directed to the misappropriation of one's image.⁵¹

In conclusion, although privacy has been recognised in New Zealand common law as a 'silent value' from early on, a tort of public disclosure of private facts has only recently been developed by the judiciary in New Zealand. This tort is limited to publications that are 'highly offensive' to an objective reasonable person. The protection of privacy in tort law is not significant from a data protection perspective, since data protection does not only involve the disclosure of personal information in a manner that is 'highly offensive'. Data protection also involves the non-offensive collection, storage, use and transmission of personal information.

2.3 Constitutional protection of privacy

New Zealand does not have a codified constitution. It does, however, have several constitutional documents, one of which is the *Bill of Rights Act* of 1990.⁵² It was adopted to implement in New Zealand law the United Nations

comes within the ambit of this tort.

50 See *Hosking v Runtig* [2005] 1 NZLR 1 32 (CA).

51 *Ibid* 42.

52 The Act is often referred to in literature as NZBORA (New Zealand Bill of Rights Act). Other constitutional documents include the *Treaty of Waitangi* of 1840, the *Statute of Westminster Adoption Act* of 1947, the *Constitution Act* of 1986, and the *Supreme Court Act* of 2003. This latter created the Supreme Court of New Zealand, which is now the court of last resort. Until 2004, appeals were possible to the Privy Council in London.

International Covenant on Civil and Political Rights.⁵³ The *Bill of Rights Act* does not have an express provision protecting privacy,⁵⁴ despite the fact that the International Covenant on Civil and Political Rights protects privacy in article 17.⁵⁵ Nevertheless, as pointed out by the Law Commission,⁵⁶

notwithstanding the unaffirmed status of privacy, considerations of privacy potentially arise in certain New Zealand Bill of Rights Act enquiries:

- under section 5 (as a justifiable limitation on affirmed rights and freedoms); and
- under section 21 (protection from unreasonable search and seizure by State enforcement agencies).

Privacy is implicitly protected by section 21 of the *Bill of Rights Act*, which provides that

[e]veryone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

The courts have held that this section protects a reasonable expectation of privacy during search and seizure.⁵⁷

Privacy can also be considered under section 5 of the *Bill of Rights Act*, which provides that

53 UN International Covenant on Civil and Political Rights (GA Res 2200A (XXI) of 16 December 1966). It entered into force on 23 March 1976.

54 The reason why privacy was not enacted in the *Bill of Rights Act* was that at the time the right to privacy was considered to be too vague and uncertain. In the White Paper commentary on the search and seizure clause, it was said that “it would be inappropriate to attempt to entrench a right that is not by any means fully recognised now, which is in the course of development, and whose boundaries would be uncertain and contentious” (see NZ Department of Justice White Paper at 104, as quoted in NZLC SP 19 at 97).

55 International Covenant on Civil and Political Rights, *supra* n 53, art 17 provides as follows:
(1) No one shall be subjected to arbitrary or unlawful interference with his [or her] privacy, family, home or correspondence, nor to unlawful attacks on his [or her] honour and reputation.
(2) Everyone has the right to the protection of the law against such interference or attacks.

56 NZLC SP 19 at 92.

57 *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA); *R v Fraser* [1997] 2 NZLR 442 (CA).

the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

It has been held, for example in *Hosking v Runting*,⁵⁸ that privacy can be a justifiable limitation imposed on freedom of expression,⁵⁹ a right which is expressly protected by the *Bill of Rights Act*.⁶⁰

The fact that privacy is recognised as a justifiable limitation on affirmed constitutional rights, such as the right to freedom of expression, is significant from a data protection perspective. Where a data protection provision overlaps with a constitutionally recognised right or freedom, such as freedom of expression, it does not necessarily mean that the data protection provision has to give way to the constitutional right or freedom. Rather, a balancing of the two competing values has to take place.

2.4 Statutory protection of privacy

Several statutes protecting privacy in specific, targeted areas have been adopted in New Zealand since the mid-1970s.⁶¹ In chronological order, reference can be made to the *Private Investigators and Security Guards Act* of 1974,⁶² which makes it an offence for a private detective to photograph, film or videotape a person or record a person's voice without that person's consent. The first *Broadcasting Act* was introduced in 1976. This Act provided that the Broadcasting Corporation of New Zealand was responsible for maintaining standards in broadcasting acceptable to the community. One of the values it

58 [2005] 1 NZLR 1 (CA).

59 Not all judges are in agreement on this. The dissenting judges in *Hosking* argued that privacy was in the nature of a value only which should not trump the right of freedom of expression. *Hosking v Runting* [2005] NZLR 1 63 (CA). See also *Brooker v Police* [2007] NZSC 30.

60 S14 of the NZ *Bill of Rights Act* of 1990 provides as follows: "Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form."

61 See NZLC SP 19 par 4.33, 4.37, 4.55.

62 S 52.

was to consider was the privacy of the individual.⁶³ The *Human Rights Act* of 1977⁶⁴ gives the Human Rights Commission monitoring functions in relation to privacy: it can report to the Prime Minister matters of concern about privacy, invite representations from members of the public, and so on. The *Crimes Act* of 1961 was amended in 1979 to add a new Part 9A in which “crimes against personal privacy” are described. The *Family Proceedings Act* of 1980 protects the privacy of individuals in divorce proceedings by providing that dissolution of marriage cases are to be heard in closed court and that publication of the proceedings is permitted only by an order of the court.⁶⁵ The *Official Information Act* of 1982 protects the privacy of the individual while making information held by government organisations available to the public.

A statute of particular significance for privacy protection is the *Broadcasting Act* of 1989. This Act replaces the earlier *Broadcasting Act* of 1976. It provides that all broadcasters must maintain standards in their programming which are acceptable to the community.⁶⁶ Among other things, they must maintain standards which are consistent with the privacy of the individual.⁶⁷ Broadcasters cannot be held liable in terms of civil law for breaches of the Act,⁶⁸ but complaints are heard by the Broadcasting Standards Authority (BSA), an independent body set up in terms of the Act.⁶⁹

63 Ss 24 and 96 *Broadcasting Act* of 1976.

64 S 67.

65 S 159. See also the *Care of Children Act* of 2004 that protects the privacy of children in court proceedings.

66 S 4(1) *Broadcasting Act* of 1989.

67 *Ibid* s 4(1)(c). Standards must also be consistent with good taste and decency; with the maintenance of law and order; with the principle that when controversial issues of public importance are discussed, reasonable efforts are made, or reasonable opportunities are given, to present significant points of view, either in the same programme or in other programmes within the period of current interest; with any approved code of broadcasting practice applying to the programmes (s 4(1)(a), (b), (d) and (e)).

68 *Ibid* s 4(3).

69 *Ibid* s 20. If the BSA finds that its standards have been breached, it can award compensation up to \$5 000 (s 13).

The BSA has formulated a set of principles to be applied to privacy complaints. Eight principles have been formulated to date.⁷⁰ The principles state that the disclosure of private facts, or public facts that have become private again (for example because of lapse of time), is inconsistent with an individual's privacy if such disclosure is highly offensive to an objective, reasonable person. The public disclosure of private facts that have been obtained by means of an intrusion into an individual's solitude and seclusion is also inconsistent with the privacy of the individual if the intrusion was highly offensive to an objective reasonable person. There is a 'public place' exemption to the last-mentioned principle, allowing the recording, photography or filming of a person in a public place. However, this exemption does not apply if the individual is particularly vulnerable and the publication would be highly offensive to an objective, reasonable person. It is a defence against a privacy complaint that the individual has consented to the publication. However, where the privacy of a child under the age of 16 is involved it is not sufficient for broadcasters to obtain informed consent. They must also satisfy themselves that the child's best interest is served by the publication. It is also a defence against a privacy complaint that the disclosure was made in the public interest. Public interest is defined as "of legitimate concern or interest to the public".⁷¹

These principles go further than the common law tort of publication of private facts, since they also consider conduct that is an intrusion into privacy as inconsistent with the privacy of the individual.⁷²

The BSA hears about 20 complaints a year and, according to the New Zealand Law Commission, has built up a substantial jurisprudence in the application of these principles. It is therefore to be expected that the courts will turn to these decisions, even if they are not binding precedents.⁷³ This Act is therefore

70 These principles can be found at BSA <http://www.bsa.govt.nz> 24 Nov.

71 *Ibid.*

72 Refer back to par 2.1 above.

73 NZLC SP 19 par 8.62.

significant for privacy law in general, since it plays a role in the development of privacy jurisprudence.

2.5 The Privacy Act of 1993

2.5.1 Introduction

In the mid-1960s various parts of the New Zealand government recognised the benefits of having a large computer system which could be used by different agencies. Plans to develop the Wanganui Computer Centre and allow agencies to have routine access to information held by other agencies caused public concern. The common law did not provide for the protection of the privacy of personal information and it was therefore necessary for the government to step in and pass the *Wanganui Computer Centre Act* of 1976. This Act set out the types of information that any one agency was allowed access to. Other agencies had to be authorised under the Act to have access to that specified information. In 1991 the office of the Privacy Commissioner was established by the *Privacy Commissioner Act* of 1991. The Privacy Commissioner's key function was to oversee data matching between the different government agencies.

This last-mentioned Act was followed by the *Privacy Act* of 1993. The *Privacy Act* repealed the *Wanganui Computer Act* as well as the *Privacy Commissioner's Act*.

The *Privacy Act* of 1993 does not, as its name perhaps suggests, create a general right to privacy. The *Privacy Act* is a data protection Act. The aim of the Act is to promote and protect individual privacy in accordance with the data protection guidelines of the Organisation for Economic Cooperation and Development (OECD),⁷⁴ of which New Zealand is a member. The OECD *Guidelines*,⁷⁵ the first international statement on data protection, were adopted

74 Also see par 1.1 above.

75 OECD *Recommendation of the Council Concerning Guidelines Governing the Protection*
76/184

in 1980. They advocate the adoption of good data protection practices to prevent unnecessary restrictions on trans-border data flows.⁷⁶

In discussing the Act we will first establish its scope of application. Then three aspects which are central to the Act's application⁷⁷ will be looked at: the information privacy principles, the role of the Privacy Commissioner, and the codes of practice.

2.5.2 *Scope of the Act*

The Act regulates the collection, use and disclosure of personal information. The Act draws no distinction between automatic and non-automatic processing activities.⁷⁸ The Act therefore equally applies to both types of processing.

The scope of the Act is to a large extent determined by the various definitions that can be found in section 2(1) of the Act. Personal information is defined as "information about an identifiable individual" and it includes "information that relates to a death" that is "maintained pursuant to the Births, Deaths, and Marriages Registration Act of 1995". An individual is defined as "a natural person, other than a deceased natural person". The effect of these two definitions is that the Act protects the information only of natural persons and that juristic persons are not protected. Further, a deceased person's personal information is not protected, but the fact that a person is deceased is seemingly protected!

Public and private sector agencies are alike subject to the privacy protection principles. This is evident from the definition of an agency as "any person or body of persons ... whether in the public sector or in the private sector". A

of Privacy and Transborder Flows of Personal Data Paris, 23 September 1980.

76 For a discussion of the OECD's data protection guidelines, see Roos *Data (Privacy) Protection* 155-173.

77 See Mount 1992-1995 *Auckland University L Rev* 410.

78 In this article the collective term 'processing activities' is sometimes used to refer to 'collection, use and disclosure'.

number of institutions or bodies are excluded from the definition of agency, such as the Sovereign, the Parliament, a court in its judicial functions, a commission of inquiry and so on. An important exemption from the definition of 'agency' is the one made for the news media in relation to its news activities. This means that the information privacy principles do not apply to the news media when it is gathering or reporting news. The Act defines a news medium as any agency whose business, or part of whose business, consists of a news activity. This exemption, according to Tobin,⁷⁹ confirms the paramount importance that the dissemination of news and current affairs has in a democracy.

Apart from the definitional section of the Act, one also has to look at specific exemptions made by the Act in order to determine its scope. Three exemptions are made from the privacy principles. First, if the Commissioner has authorised, in terms of section 54 of the Act, the collection, use or disclosure of the information, the processing activities are exempt from some of the information privacy principles.⁸⁰ Secondly, if the information is of a certain type listed in the Act,⁸¹ it is exempted from the access and rectification principles.⁸² Thirdly, if it is information kept by individuals for purely personal, home or family purposes, it is exempted from all of the principles.⁸³

79 Tobin "Privacy and Freedom of Expression" 136.

80 According to the NZ Privacy Commissioner, "section 54 of the Privacy Act allows the Commissioner to authorise actions that would otherwise be a breach of principles 2, 10 or 11. The power to grant specific exemptions gives the Act extra flexibility by taking account of unanticipated collection, use or disclosure of information that is in the public interest or in the interests of the person concerned. Section 54 can be useful when some disclosure ought to be made in the public interest but there is a duty under the Act not to disclose and the agency has not formulated a clear policy enabling disclosure. It can also act as a 'safety valve' to address rare and unexpected problems." See NZ Privacy Commissioner *Annual Report 2007* <http://www.privacy.org.nz/> 27 Nov, at 29.

81 Namely, personal information in the course of transmission by post, telegram, cable, facsimile transmission, electronic mail and other similar means of communication; evidence given to a commission of inquiry or in a court, communication between the office of the Ombudsman and an agency, or between the Commissioner and an agency (*Privacy Act of 1993* s 55(a)-(e)).

82 *Privacy Act of 1993* s 55.

83 *Ibid* s 56.

This last-mentioned exemption is found in many of the recent data protection instruments.⁸⁴ The rationale is that this type of processing (eg, the collection and storing of names and telephone numbers of friends and family members) does not create a serious threat of privacy infringement. This is true, as long as the individual collecting the information does not place it on the internet and make it available to more persons than his or her family!⁸⁵

2.5.3 Information privacy principles

The twelve information privacy principles are the mainstay of the Act. Information privacy principles, also referred to as data protection principles or fair information principles, are found in one form or another in most data protection instruments.⁸⁶ The aim of data protection principles is to ensure that the processing of personal information is done lawfully and fairly towards the data subject (that is, the individual whose personal information is processed).

Looking at how the principles in the *Privacy Act* are formulated, it is evident that the *Privacy Act* distinguishes between the different stages of data processing. The Act has principles that relate to the collection, to the storage, to the use or to the disclosure of personal information. In this regard the *Privacy Act* can be improved. The trend among more recent data protection Acts (such as the UK *Data Protection Act* of 1998) is no longer to distinguish between the different stages of processing but to refer only to the 'processing' of information. The reason is that, in the modern online environment, the distinction between collecting, storing, processing and transfer of data becomes blurred. It is therefore more sensible to regulate the 'processing' of personal data. Processing refers to almost any action that can be performed on personal information.⁸⁷

84 See, eg, the data protection Acts of the UK (the *Data Protection Act* of 1998 s 36) and of the Netherlands (*Wet Bescherming Persoonsgegevens* of 2000 art 2(2)(a)).

85 Social networking sites such as MySpace or Facebook allow an individual to put the information of friends and family on his or her web page.

86 See further Roos 2006 *CILSA* 107 *et seq.*

87 *Ibid* 105.

The information privacy principles of the *Privacy Act* do not override other laws which govern the collection, use or disclosure of personal information.⁸⁸ All of the information privacy principles are found in section 6 of the Act.⁸⁹ All of the first four, (1) "Purpose of collection of personal information", (2) "Source of personal information", (3) "Collection of information from subject" and (4) "Manner of collection of personal information", deal with the collection stage of data processing.⁹⁰ Principle 1 directs an agency to collect personal information only for a lawful purpose that is connected with a function of the agency, and only if that collection is necessary for that purpose. As will be indicated, the purpose for which the information is collected plays an important role in many of the other principles. Principle 2 provides that information must be collected directly from the individual concerned, unless specific exceptions are present.⁹¹ Principle 3 requires that the agency must take reasonable steps, at the time of collection of the information, to inform the individual of certain matters, such as the fact that the collection of the information is taking place, the purpose for which it is collected, the intended recipients of the information, the names and addresses of the persons who are collecting the information, and who will hold it. The individual should also be informed whether the information is collected under authority of a specific law, whether or not the provision of the information is mandatory, the consequences if the individual fails to provide all the information, and also of the individual's right to access and request correction of data. An agency is not required to take these steps if they have already done

88 S 7 *Privacy Act* of 1993.

89 It is therefore not useful to give a footnote reference for each separate principle.

90 S 6 *Privacy Act*, principles 1-4.

91 The exceptions are when the agency collecting the information believes on reasonable grounds as follows: that the information is publicly available; or that the individual concerned authorises collection of the information from someone else; or that the interests of the individual concerned are not prejudiced; or that it is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or that complying with this principle would prejudice the purposes of collection; or that complying with this principle would not be reasonably practical in the particular case; or that the information will not be used in a form that identifies the individual; or that the Privacy Commissioner has authorised collection under s 54.

so in relation to the same personal information, or information of the same kind, on a recent, previous occasion. Other exemptions from the duty to inform the individual are also available in particular circumstances.⁹² Principle 4 provides that personal information may not be collected by unlawful means or in a manner that is unfair or intrudes unreasonably into the individual's personal affairs.

Principle 5 ("Storage and security of personal information") directs that the agency that holds the information must take reasonable security measures to ensure that there are reasonable safeguards against loss, misuse or disclosure. If it is necessary to give information to another person, such as someone working on contract, everything reasonable must be done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 ("Access to personal information") and principle 7 ("Correction of personal information") provide that the individual has a right to obtain confirmation from the agency whether it holds information on him or her, to have access to such information and to request correction of incorrect information. If agencies have already passed on personal information that they then correct, they should inform the recipients about the correction. The Act makes detailed provision for the manner in which the rights to access and correction should be exercised.⁹³ The Act limits the right to request access to an individual who is a New Zealand citizen, a permanent resident of New Zealand or an individual who is in New Zealand.⁹⁴ The Act provides for several exemptions, *inter alia* relating to security, prevention and detection of crime and the safety of individuals, from the right to access personal data.⁹⁵

92 Namely, if the information is publicly available; if the collection has been authorised by the individual; if it is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or if compliance is not reasonably practicable in the particular case; or if the information will not be used in a form in which the individual concerned is identified.

93 Ss 33-45 (Part 5) *Privacy Act of 1993*.

94 *Ibid* s 34.

95 Access to information may be refused for a range of reasons, including the fact that

Once information has been collected, the Act provides in principle 8 (“Accuracy, etc, of personal information to be checked before use”) that the agency must take steps that are reasonable in the circumstances to ensure that the information is accurate, up-to-date, complete, relevant and not misleading, before it is used or disclosed. These qualities have to be determined with reference to the purpose for which it was collected, because information that may be relevant, complete or up-to-date for one purpose might be irrelevant, incomplete or outdated for another.

Principle 9 (“Agency not to keep personal information for longer than necessary”) provides that information may not be kept for longer than is necessary for the purpose for which it was collected. Principle 10 (“Limits on the use of personal information”) limits the use of the collected information to the purpose for which it was collected. Information may be used for a different purpose from the one it was collected for only if the agency believes on reasonable grounds that one of several situations listed in the Act which allows the different use is applicable.⁹⁶

access would pose risks to New Zealand’s security or defence, breach confidences with another government, prevent detection of criminal offences or the right to a fair trial, endanger the safety of an individual, disclose a trade secret or unreasonably prejudice someone’s commercial position, involve an unwarranted breach of another individual’s privacy, breach confidence where the information has been gained solely for reasons to do with the individual’s employment or to decide whether to insure the individual, be contrary to the interests of an individual under the age of 16, breach legal professional privilege, reveal the confidential source of information provided to a Radio New Zealand or Television New Zealand journalist, or constitute contempt of court or the House of Representatives (*Ibid* ss 27-32 [Part 4]).

⁹⁶ Namely, if the use is one of the purposes for which the information was collected; or the use is directly related to the purpose the information was obtained for; or the agency got the information from a publicly available publication; or the individual concerned has authorised the use; or the use is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or the use is necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life or health of any individual; or the individual concerned is not identified; or the use is authorised by the Privacy Commissioner under s 54 of the Act.

Principle 11 (“Limits on disclosure of personal information”) provides that personal information may be disclosed only in certain limited situations listed in the Act.⁹⁷

Principle 12 (“Unique identifiers”) is new, in the sense that it is not found in the OECD *Guidelines* on which the *Privacy Act* is based. It regulates the use of unique identifiers, such as bank customer numbers, driver’s licence and passport numbers. These identifiers must not be assigned to individuals unless this is necessary for the organisation concerned to carry out its functions efficiently. The identifiers must be truly unique to each individual (except in some tax-related circumstances) and the identity of individuals must be clearly established. No one is required to disclose their unique identifier unless it is for or related to one of the purposes for which the identifier was assigned. It follows from this that the Government is not allowed to give people one personal number to use in all of their dealings with government agencies.⁹⁸ This prevents the linking of files (also referred to as information matching)⁹⁹ from different agencies by means of the same unique identifier.¹⁰⁰

97 The agency may disclose information only if the agency reasonably believes that the disclosure is in connection with, or directly related to, one of the purposes for which it was obtained; or the agency got the information from a publicly available publication; or disclosure is to the individual concerned; or disclosure is authorised by the individual concerned; or it is necessary for a public sector agency to disclose the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life or health of any individual; or disclosure is necessary to facilitate the sale of a business as a going concern; or the information is to be used in a form in which the individual concerned is not identified; or disclosure has been authorised by the Privacy Commissioner under s 54.

98 See NZ Privacy Commissioner Fact Sheet no 2 <http://www.privacy.org.nz> 18 Jun.

99 Information matching, data matching, computer matching or record linkages entail 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 programme. The aim of these programmes is usually to eliminate fraud, waste and abuse from government programmes, but a side-effect could be that the government builds up dossiers about individuals. See Flaherty, *supra* n 12, 344. See also Borking “Privacy Technology” 97; Madsen *Personal Data Protection* 12; Turkington and Allen *Privacy Law* 313.

100 The public sector may make use of information matching, but only within the limits of the *Privacy Act* of 1993. The Commissioner must examine proposed legislation that makes provision for information matching and must report to the responsible Minister the results

The *Privacy Act* also contains four public register privacy principles which limit the following: the manner in which information can be made available from public registers, the re-sorting or combining of public register information for commercial gain, the electronic transmission of public registers, and the charging for access to public register information.¹⁰¹

A data protection principle found in other data protection instruments,¹⁰² which is absent in the *Privacy Act*, is the principle that personal information that is considered to be 'sensitive' should be subject to more stringent controls than non-sensitive personal information.¹⁰³ This principle is manifested primarily in rules that place special limits on the processing of predefined categories of data.¹⁰⁴ Information that is considered 'sensitive' is information on a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and sexual life.¹⁰⁵ It is suggested that the *Privacy Act* can be improved by incorporating a sensitivity principle.

of the examination. Part 10 of the Act (ss 97-109) contains specific provisions to regulate information matching. All authorised information matching programmes are listed in sch 3 of the Act. Sch 4 contains rules that must be complied with when authorised matching takes place. S 105 of the *Privacy Act* requires an annual report on each authorised matching programme carried out in that year.

101 *Ibid* s 59.

102 See, eg, s 2 UK *Data Protection Act* of 1998.

103 The reason why the *Privacy Act* does not contain this provision is that such a provision is absent in the OECD *Guidelines* on which the New Zealand legislation is based. The Group of Experts, drafting the OECD *Guidelines*, could not reach consensus on which categories of data deserve special protection. It was confronted by two opposing views as regards the enumeration of sensitive data. One view, which was supported by European legislatures, was that it is both possible and desirable to enumerate types of data which are intrinsically sensitive, with the result that the collection of these types of data should be prohibited or at least restricted. Examples of such sensitive data are data that relate to race, religious beliefs and criminal records. The other view, support for which may be found in the privacy legislation of the USA, the *Privacy Act* of 1974, was that no data were intrinsically sensitive or private, but become so as a result of their context and use. In the end the Group of Experts found it impossible to define any set of data which was universally regarded as sensitive, and consequently only formulated a general criterion that there should be limits to the collection of personal data. The nature of the limits to the collection of data is not spelt out, but in the OECD *Guidelines* 29 it is envisaged that the limits relate *inter alia* to the 'earmarking' of especially sensitive data according to traditions and attitudes in each member country. See also Bygrave, *supra* n 2, 69.

104 See further Roos, *supra* n 86, 121; Bygrave, *supra* n 2, 68-69.

105 Art 8(1) Dir 95/46/EC.

2.5.4 Oversight and enforcement of the Act: the Privacy Commissioner and Human Rights Review Tribunal

The Commissioner can be thought of as the 'statutory guardian' of the *Privacy Act*.¹⁰⁶ One of the most important functions of the Commissioner is to receive complaints. An individual who feels aggrieved by an interference with his or her privacy under the Act¹⁰⁷ may lodge a complaint with the Privacy Commissioner.¹⁰⁸ An individual does not, for the most part, have recourse to the courts for a breach of an information privacy principle. In terms of the Act, only the entitlement to access data held by a public sector agency can be enforced in a court of law.¹⁰⁹ None of the other information privacy principles confers legal rights enforceable in a court of law.¹¹⁰

Once a complaint has been lodged, the Privacy Commissioner can respond in several ways. It may be decided not to investigate the matter, if the complaint is trivial or vexatious or otherwise unworthy of investigation.¹¹¹ If this is not the case, the Commissioner must investigate the matter and act as a conciliator (or

¹⁰⁶ See Mount, *supra* n 77, 411.

¹⁰⁷ In terms of s 66 of the *Privacy Act*, an action is an interference with the privacy of the individual for the purposes of a complaint under the *Privacy Act*, "if, and only if,—

- (a) In relation to that individual—
 - (i) The action breaches an information privacy principle; or
 - (ii) The action breaches a code of practice issued under section 63 of this Act (which relates to public registers); or
 - (iii) The provisions of Part 10 of this Act (which relates to information matching) have not been complied with; and
- (b) In the opinion of the Commissioner or, as the case may be, the Tribunal, the action—
 - (i) Has caused, or may cause, loss, detriment, damage, or injury to that individual; or
 - (ii) Has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or
 - (iii) Has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual."

¹⁰⁸ *Ibid* s 67.

¹⁰⁹ *Ibid* s 11(1).

¹¹⁰ *Ibid* s 11(2). This is not necessarily a weakness in the *Privacy Act*, since the Act does provide for independent adjudication and for compensation to be paid and sanctions imposed where appropriate. These functions are performed by the Human Rights Review Tribunal (*ibid* s 71(2)).

¹¹¹ *Ibid* s 71.

mediator) in the matter.¹¹² The Commissioner may, in order to settle the matter, call a compulsory conference between the parties to the complaint.¹¹³

The Commissioner may also decide to refer the complaint, where appropriate, to another body such as an Ombudsman, the Health and Disability Commissioner or the Inspector-General of Intelligence and Security.¹¹⁴ In some cases the matter may be taken further, to the Human Rights Review Tribunal.¹¹⁵ The Tribunal may give the relief that it thinks is suitable. This may include a declaration that there is an interference with the privacy of the plaintiff, damages, or an order either prohibiting or compelling certain action on the part of the defendant.¹¹⁶

The Commissioner has several other functions in terms of the Act. A few of these functions can be listed by way of example.¹¹⁷ The Commissioner must promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles; must monitor and report on the use of unique identifiers; must maintain and publish directories of personal information;¹¹⁸ and must examine any proposed legislation that makes provision for the collection of personal information by a public sector agency, or the disclosure of personal information by one public sector agency to another public sector agency. The Commissioner may inquire generally into any matter, enactment, law, practice or procedure, or any technical development, that appears to infringe the privacy of the individual and

112 *Ibid* s 69(1).

113 *Ibid* s 76.

114 *Ibid* ss 72, 72A and 72B.

115 *Ibid* s 71(2).

116 *Ibid* s 85.

117 See further *ibid* s 13.

118 In terms of s 21 *Privacy Act* of 1993. The Commissioner may from time to time publish one or more publications that include information on the nature of and the purpose for which personal information is held, the classes of individuals about whom personal information is held, the period for which any type of personal information is held, the individuals who are entitled to have access to the personal information and the conditions under which they are entitled to have that access, and the steps that should be taken by any individual wishing to obtain access to personal information held by an agency.

may undertake research into and monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised. He or she may report to the responsible Minister the results of such research and monitoring, may examine any proposed legislation that may affect the privacy of individuals, and may report to the Prime Minister from time to time on the desirability of the acceptance, by New Zealand, of any international instrument relating to the privacy of the individual.

2.5.5 Codes of practice

The Privacy Commissioner has the power to issue codes of practice that become law.¹¹⁹ Codes of practice are sometimes also referred to as codes of conduct. The purpose of a code of conduct (or code of practice) is to translate the legislative provisions into a practical application in the specific information sector involved.

The effect of a code issued under the *Privacy Act* is that it modifies the operation of the Act for a specific industry, agency, activity or type of personal information.¹²⁰ Codes often modify one or more of the information privacy principles by prescribing standards that are either more or less stringent.¹²¹ In this way account can be taken of special circumstances which affect a class of agencies (such as credit reporters) or a class of information (such as health information).¹²²

Codes of practice are issued by the Commissioner, either after receiving proposals for a code by a representative body of a particular class of agency or

119 *Ibid* s 46(1).

120 *Ibid* s 46(3).

121 *Ibid* s 46(2).

122 At present, codes of practice have *inter alia* been adopted for the credit reporting industry, the health information industry and the telecommunications industry. See the Privacy Commissioner's website at <http://www.privacy.org.nz>.

industry, or on the Commissioner's own initiative.¹²³ Codes of practice can be amended or revoked by the Commissioner.¹²⁴ This makes them a flexible means of regulation.

Codes of practice are deemed to be regulations,¹²⁵ which mean that they must be presented to the House of Representatives.

2.5.6 Conclusion

In general, it can be said that New Zealand has a data protection regime that functions well. The *Privacy Act* of 1993 allows individuals to have a measure of control over the processing of their personal information.¹²⁶ The Commissioner fulfils a conciliatory function and complaints are resolved without the need for expensive litigation.¹²⁷

New Zealand's data protection law goes a long way to providing adequate data protection as required by the EU Directive on data protection.¹²⁸ The EU has not made a finding to that effect, however. According to the Privacy Commissioner, the "Privacy Act requires a couple of amendments before New Zealand might be adjudged 'adequate'".¹²⁹ The following two amendments are considered necessary:

- (1) The Act should include a provision that restricts trans-border movement of personal data. In other words, once personal information is imported into New Zealand, there should be a provision

123 *Ibid* s 47.

124 *Ibid* s 51.

125 *Ibid* s 50.

126 During 2006-2007 the Commissioner's office received 640 privacy complaints. About two-thirds of those complaints were about access to personal information or disclosure of personal information.

127 Many complaints are resolved without the need of escalating them to the Tribunal. According to the NZ Privacy Commissioner *Annual Report 2007* "[o]f the 701 complaints closed in 2006/07, 75% (524) were successfully settled without needing to proceed to a final opinion" (*supra* n 80, 7).

128 See NZLC SP 19 par 4.53.

129 See Shroff "Privacy and Sovereignty" 9.

in the *Privacy Act* prohibiting the further transfer of the data to a country which does not provide adequate data protection. A provision similar to section 25 of the EU Directive is needed to remedy this shortcoming.¹³⁰

- (2) The restrictions on the right to request access should be removed. As seen, at present only New Zealand citizens, permanent residents and individuals present in New Zealand may make a request for access.¹³¹

3 South African law

3.1 Introduction

Although the scope of the article does not permit an extensive discussion of the South African position,¹³² it is necessary to familiarise the reader with the current situation in South Africa before any recommendations can be made based on the New Zealand experience.

3.2 Protection of privacy and identity in common law

The processing of data can infringe on a person's personality primarily in two ways: where true personal information is processed, a person's privacy is infringed, and where false or misleading information is processed, the person's identity is infringed.¹³³ Privacy and identity are personality interests that are protected in the law of delict by the *actio iniuriarum*.¹³⁴ With this action satisfaction is claimed for the wrongful, intentional interference with a

130 Art 25(1) Dir 95/46/EC provides as follows: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

131 S 34 *Privacy Act* of 1993.

132 See Roos, *supra* n 2, for a discussion of the current SA position against the background of international standards in data protection.

133 Neethling, Potgieter and Visser *Law of Personality* 270-271.

134 *Ibid* 29, 36, 39.

personality interest.¹³⁵ Patrimonial loss that flows from the wrongful, negligent infringement of the personality can be claimed with the *actio legis Aquiliae*.¹³⁶ An interdict is also available to avert an impending interference with the right to privacy or identity, or to prevent the continuation of a wrongful infringement.¹³⁷

At common law, privacy has been recognised since the mid-1950s as a separate personality interest worthy of protection: *O’Keeffe v Argus Printing and Publishing Co Ltd*¹³⁸ is regarded as the *locus classicus* for the recognition of an independent right to privacy in South African law.¹³⁹ Other cases followed *O’Keeffe* in which the right to be free from the public disclosure of private facts¹⁴⁰ and the right to be free from unreasonable intrusions into the private sphere¹⁴¹ were recognised.¹⁴² Both individuals and juristic persons are entitled to a right to privacy.¹⁴³

Neethling’s¹⁴⁴ definition of privacy as “an individual condition of life characterised by seclusion from the public and publicity ... [which] condition embraces all those personal facts which the person concerned has himself [or herself] determined to be excluded from the knowledge of outsiders and in respect of

135 Neethling, Potgieter and Visser *Law of Delict* 5.

136 Neethling, Potgieter and Visser *Law of Personality* 67.

137 Neethling, Potgieter and Visser *Law of Delict* 237.

138 1954 3 SA 244 (C).

139 See Neethling, Potgieter and Visser *Law of Personality* 217.

140 Eg *Mhlongo v Bailey* 1958 1 SA 370 (C) (unauthorised publication of a photograph of a retired schoolteacher portraying him as a young man in the company of a well-known singer); *Rhodesian Printing and Publishing v Duggan* 1975 1 SA 590 (R) (a story about young children abducted from the custody of their parents); *La Grange v Schoeman* 1980 1 SA 885 (E) (attempted photographing of security policemen described by counsel at a trial as having been responsible for the death of a detainee).

141 Eg *Gosschalk v Rossouw* 1966 2 SA 476 (C) 492 (improperly interrogating a detainee); *S v A* 1971 2 SA 293 (T) (electronically bugging a person’s home).

142 Recent cases in which the former Appellate Division (now the Supreme Court of Appeal) also recognised and discussed the right to privacy include *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A), *National Media v Jooste* 1996 3 SA 262 (A) *Financial Mail v Sage Holdings* 1993 2 SA 451 (A) and *Janit v Motor Industry Fund Administrators* 1995 4 SA 293 (A).

143 *Financial Mail v Sage Holdings* 1993 2 SA 451 (A) 462-463; *Motor Industry Fund v Janit* 1994 3 SA 56 (W) 60-61; *Janit v Motor Industry Fund Administrators* 1995 4 SA 293 (A) 304. See also *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 1 SA 545 (CC) 557.

144 Neethling, Potgieter and Visser *Law of Personality* 32.

which he [or she] has the will that they be kept private” has been accepted by the South African courts.¹⁴⁵

Since privacy relates to personal facts which a person has determined should be excluded from the knowledge of outsiders, it follows that privacy can be infringed only when someone learns of true private facts about the person against his or her determination and will.¹⁴⁶ Such knowledge can be acquired in one of two ways:¹⁴⁷ (1) where an outsider himself or herself learns of the facts (such interference with privacy is referred to as intrusion or acquaintance),¹⁴⁸ or (2) where an outsider acquaints third parties with personal facts which, although known to the outsider, nonetheless remain private (such interference with privacy is referred to as disclosure or publicity).¹⁴⁹

Privacy must be distinguished from identity. Identity is defined as “a person’s uniqueness or individuality which identifies or individualises him [or her] as a particular person and thus distinguishes him [or her] from others”.¹⁵⁰ Identity is infringed when the personality image of a person is falsified. Two of the torts recognised by Prosser as an infringement of the right to privacy¹⁵¹ can be classified as infringements of the right to identity, namely “publicity which places the plaintiff in a false light” and “appropriation for the defendant’s advantage, of the plaintiff’s name or likeness”.¹⁵²

145 See, eg, *National Media v Jooste* 1996 (3) SA 262 (A) 271-272.

146 Neethling, Potgieter and Visser *Law of Delict* 33.

147 *Ibid* 322; Neethling, Potgieter and Visser *Law of Personality* 33; *Motor Industry Fund Administrators v Janit* 1994 3 SA 56 (W) 60; *Bernstein v Bester* 1996 2 SA 751 (CC) 789. Compare *Financial Mail v Sage Holdings* 1993 2 SA 451 (A) 462- 463; also see McQuoid-Mason *Privacy* 134.

148 Eg by unlawfully intruding on property, searching and seizing documents, secretly watching someone or using surveillance equipment to gather information on someone (see *S v A* 1971 2 SA 293 (T)).

149 An example of an acquaintance through disclosure is when a doctor tells his friends about a patient’s HIV status (see *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A)).

150 Neethling, Potgieter and Visser *Law of Personality* 36.

151 See par 2.2 above.

152 Neethling, Potgieter and Visser *Law of Personality* 37.

Identity was described as an independent personality interest worthy of delictual protection in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*,¹⁵³ but until 2007 this interest was usually protected in case law under the guise of other personality interests, such as the right to a good name and the right to privacy.¹⁵⁴ However, in 2007 the Supreme Court of Appeal in *Grutter v Lombard*¹⁵⁵ gave recognition to identity as a separate personality interest. The court held that a person's name as a feature of his or her right to identity constitutes an interest that is capable of legal protection. According to the court, a person's interest in preserving his or her identity against unauthorised exploitation is encompassed by the concept of *dignitas*, which incorporates both identity and privacy. The court confirmed that infringements of these interests are considered *iniuriae* in South African law and, as such, covered in terms of both liability and remedies by the law of delict.¹⁵⁶

Although South Africa has a well-developed level of protection for the right to privacy and identity in the law of delict, this is not sufficient to provide adequate data protection. The traditional delictual principles provide only limited protection for the individual's personal information. Delictual principles do not give the individual active control over personal information that is being processed.¹⁵⁷ The traditional principles are useful to determining whether or not processing of personal information has taken place lawfully. However, the traditional principles cannot ensure, for example, that the data subject has knowledge of the fact that his or her personal information has been collected, or that he or she has access to the information, or that he or she may correct incorrect information.¹⁵⁸

153 1977 4 SA 376 (T) 386.

154 See *O'Keeffe v Argus Printing and Publishing* 1954 3 SA 244 (C) and *Kidson v SA Associated Newspapers* 1957 3 SA 461 (W) (unauthorised use of a photograph for a false newspaper story).

155 2007 4 SA 89 (SCA) par [12].

156 2007 4 SA 89 (SCA) par [12]. See also Neethling 2007 *TSAR* 834.

157 See Neethling, Potgieter and Visser *Law of Personality* 278.

158 See also Roos, *supra* n 2, 423.

3.3 *Protection of privacy and identity in constitutional law*

Privacy is expressly protected in section 14 of the Constitution.¹⁵⁹ The constitutional right to informational privacy has been interpreted by the Constitutional Court as coming into play wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable.¹⁶⁰ In other words, it extends to those aspects of a person's life in regard to which he or she has a legitimate expectation of privacy.¹⁶¹ "The interest that a person has in preserving his or her identity against unauthorised exploitation" has been recognised in *Grutter v Lombard*¹⁶² as a fundamental right protected under section 10 of the Constitution, as "one of 'a variety of personal rights' that are included in the concept of *dignitas* in the context of the *actio injuriarum*". Since privacy and identity are protected as fundamental rights, this constitutional imperative obliges the government to adopt legislation for the adequate protection of information privacy, since ordinary private law principles provide only partial protection in this respect. Such principles can be introduced only by legislation and not by the courts.¹⁶³

159 S 14 provides as follows:

Everyone has the right to privacy, which includes the right not to have:

- (a) their person or home searched;
- (b) their property searched;
- (c) their possessions seized;
- (d) the privacy of their communications infringed.

160 See *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 1 SA 545 (CC) 557. See further Roos, *supra* n 2, 400. The constitutional right to privacy extends further than the delictual right to privacy, and protects interests such as autonomy also.

161 *Bernstein v Bester* 1996 2 SA 751 (CC) 792; *Protea Technology v Wainer* [1997] 3 All SA 594 (W) 608; 1997 9 BCLR 1225 (W) 1241.

162 2007 4 SA 89 (SCA) par 12.

163 There are two reasons for this. First of all, in view of the inherent conservatism of the courts it is improbable that the application of the traditional data protection principles by the courts will occur often or extensively enough in the near future (see Neethling, Potgieter and Visser *Law of Personality* 272). Secondly, the most important force behind legal reform is the legislature and not the judiciary; see *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)* 2001 4 SA 938 (CC). Since the introduction of a new data (privacy) protection regime is not merely an incremental change of the law, but a sometimes radical departure from existing law and an extensive regulation of the present field, it is a task for the legislature (Neethling 2002 *THRHR* 587).

3.4 Data protection provisions in statutory law

South Africa does not have an omnibus data protection law. Instead, we have three statutes that contain some (limited) data protection provisions, namely the *Promotion of Access to Information Act*,¹⁶⁴ the *Electronic Communications and Transactions Act*¹⁶⁵ and the *National Credit Act*.¹⁶⁶ These Acts cannot be considered as omnibus data protection laws. Even when their legal effects are considered together, they do not provide adequate data protection for all personal information processed in South Africa.¹⁶⁷

The recommendations of the South African Law Reform Commission for an omnibus data protection law for South Africa which is encapsulated in a draft Bill (the Draft Bill on the Protection of Personal Information) are as follows:¹⁶⁸

- a) Privacy and information protection should be regulated by a general information protection statute, with or without sector specific statutes, which will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. Automatic and manual processing will be covered and identifiable

164 Act 2 of 2000. This Act promotes the data protection principle of access to personal information, by permitting individuals access to both manual and computer records containing personal information about themselves (ss 11 and 50).

165 Act 25 of 2002. Ch VIII of this Act aims to address the privacy concerns of consumers by enumerating principles in s 51 that must be adhered to when a data controller electronically collects personal information. However, the Act does not impose legally binding obligations on data controllers, but provides that "a data controller may voluntarily subscribe to the principles by recording such fact in any agreement with a data subject" (s 50(2)).

166 Act 34 of 2005. This Act regulates the processing of personal information in the consumer industry. The Act provides that a person who receives, compiles, retains or reports confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information (s 68(1)). Credit bureaus have certain duties in respect of consumer credit information. They must *inter alia* take reasonable steps to verify the accuracy of such information reported to them, retain such information for prescribed periods, maintain consumer credit records in accordance with prescribed standards, and expunge information that is not permitted to be stored. They must also issue a report to any person who requires it for a prescribed purpose or a purpose contemplated in the Act and may not knowingly or negligently provide a report containing inaccurate information (s 70(2)).

167 See Roos, *supra* n 2, 424-433 for a full discussion of these Acts.

168 See SALRC *Privacy and Data Protection*, *supra* n 17, vi-vii.

natural and juristic persons will be protected [Chapter 2, clauses 3-6].¹⁶⁹

- b) General principles of information protection should be developed and incorporated in the legislation. The proposed Bill gives effect to eight core information protection principles, namely processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. Provision is made for exceptions to the information protection principles [Chapter 3, Part A, clauses 7-23]. Exemptions are furthermore possible for specific sectors in applicable circumstances [Chapter 4, clauses 32-33]. Special provision has furthermore been made for the protection of special (sensitive) personal information [Chapter 3, Part B, clauses 24-31].
- c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission [Chapter 5, Part A, clauses 34-46]. The Commission will be responsible for the implementation of both the *Protection of Personal Information Act* (see Annexure B) and the *Promotion of Access to Information Act, 2000*. Data subjects will be under an obligation to notify the Commission of any processing of personal information before they undertake such processing [Chapter 6, Part A, clauses 47-51] and provision has also been made for prior investigations to be conducted where the information being collected warrants a stricter regime [Chapter 6, Part B, clauses 52-53].
- d) Enforcement of the Bill will be through the Commission 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 Commission may furthermore assist a data subject in

169 References in brackets are to the applicable clauses, parts and chapters in the Protection of Personal Information Bill set out in Annexure B to SALRC *Privacy and Data Protection*, *supra* n 17.

claiming compensation from a responsible party for any damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence [Chapter 8, clauses 63-87 and Chapter 9, clauses 88-92].

- e) A flexible approach should be followed in which industries will develop their own codes of conduct (in accordance with the principles set out in the legislation) which will be overseen by the regulatory agency. Codes of conduct for individual sectors may be drawn up for specific sectors on the initiative of the specific sector or of the Commission itself. This will include the possibility of making provision for an adjudicator to be responsible for the supervision of information protection activities in the sector. The Commission will, however, retain oversight authority. Although the codes will accurately reflect the information protection principles as set out in the Act, it should furthermore assist in the practical application of the rules in a specific sector [Chapter 7, clauses 54-62].
- f) It is the Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Directive. In this regard a provision has been included that prohibits the transfer of personal information to countries that do not, themselves, ensure an adequate level of information protection [Chapter 10, clause 94].

These proposals contain a set of information privacy principles which, if complied with, will ensure fair and lawful processing. They provide for oversight by an independent body and remedies are made available should the data controller not comply with the provisions of the proposed Act. They specifically provide for processing that involves sensitive personal information and imposes restrictions on the onward transfer of personal data. It is submitted that these proposals, which have been in "suspended animation"¹⁷⁰ for three years, will

170 Engelbrecht 2008 <http://www.itweb.co.za/sections> 16 Jun.

provide adequate data protection as required by the EU Directive. However, as long as it remains a draft Bill it does not have any legal consequences.

4 Lessons for South Africa from the New Zealand experience

Can South Africa learn any lessons from New Zealand data protection law? We have seen that New Zealand only recently recognised a tort of publication of private facts, whereas South Africa's protection of the right to privacy is better developed and more extensive than that of New Zealand. Privacy is also expressly protected in our Constitution, whereas New Zealand's Bill of Rights Act does not list privacy as a protected right.¹⁷¹ One may be forgiven for assuming that South Africa places a higher value on the individual's right to privacy than New Zealand does. Despite all of this, New Zealand adopted a data protection Act fifteen years ago, while South Africa still has not done so.

If there is one thing we can learn from New Zealand law, it is the necessity of a data protection law. New Zealand has had its Act in place for more than fifteen years. During this time all the parties involved (individuals, agencies, the Commissioner and the Human Rights Review Tribunal) became experienced in the application of the *Privacy Act* and individuals came to understand their rights in terms thereof. Although the *Privacy Act* needs improvement, something the New Zealand legislature recognises,¹⁷² the Act in its present form already complies with most of the international standards of adequate data protection.¹⁷³

171 Refer to Roos, *supra* n 2, 421 *et seq* for a discussion of the protection of privacy under South African common law and the *Constitution of the Republic of South Africa*, 1996.

172 According to the NZLC SP 19 par 1.15, the Ministry of Justice is undertaking work on modernising the *Privacy Act* of 1993.

173 The fact that an adequate level of data protection is required by the EU Directive on data protection before personal information will be allowed to be transferred from the EU to a non-EU country is discussed by Roos 2007 SALJ 400.

Looking at the specific provisions of the New Zealand *Privacy Act* of 1993, the exemption made for the news media is worth further research, with a view to implementing a similar provision in a South African data protection Act. It is important that freedom of speech should be balanced with the right to privacy. Should South Africa decide to adopt a protection of personal information Act, it is suggested that the Act should contain a provision that maintains an appropriate balance between the protection of privacy and the protection of freedom of speech. This may, for example, mean that exemptions should be made from the data protection principles where personal data are processed solely for journalistic purposes or for the purpose of artistic or literary expression.¹⁷⁴

5 Conclusion

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.¹⁷⁵ It is suggested that South Africa can take note of the New Zealand experience, since it provides a good example of a well-functioning data protection regime. In conclusion, the South African legislature is urged to adopt the proposals of the South African Law Reform Commission as a matter of urgency.

174 See also art 9 Dir 95/46/EC.

175 See Roos, *supra* n 2, 411-413 for more detail.

Bibliography

ALI *Restatement (Second) of Torts*

American Law Institute *Restatement (Second) of Torts* (American Law Institute Publishers St Paul, Minnesota 1977)

Bennett *Regulating Privacy*

Bennett CJ *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press Ithaca 1992)

Bloustein 1964 *NYULR*

Bloustein EJ "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" 1964 *New York University Law Review* 962-1007

Blume 1997 *Int R L Computers & Tech*

Blume P "Privacy as theoretical and practical concept" 1997 *International Review of Law, Computers & Technology* 193-202

Borking "Privacy technology"

Borking J "Privacy technology, a new challenge in cyberspace" in Ippel P, De Heij G and Crouwers B (eds) *Privacy Disputed* (SDU Den Haag 1995)

Burns *Communications Law*

Burns Y *Communications Law* (Butterworths Durban 2001)

Burrows "Invasion of Privacy"

Burrows J "Invasion of Privacy" in Todd S (ed) *The Law of Torts in New Zealand* 4th ed (Law Book North Ryde NSW 2005)

Bygrave 2001 *UNSWLJ*

Bygrave LA "The place of privacy in data protection law" 2001 *University of New South Wales Law Journal* 277-283

Bygrave *Data Protection Law*

Bygrave L A *Data Protection Law: Approaching its Rationale, Logic and Limit* (Kluwer Law International The Hague 2002)

Eiselen *Reg op privaatheid in die inligtingsera*

Eiselen GTS *Die reg op privaatheid in die inligtingsera* Unpublished
inaugural lecture PU vir CHE (1994)

Flaherty *Surveillance Societies*

Flaherty DH *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*
(University of North Carolina Press Chapel Hill 1989)

Korff *Data Protection Laws in the EU*

Korff D *Data Protection Laws in the European Union* (Federation of European Direct Marketing Brussels 2005)

Kuner *European Data Privacy Law*

Kuner C *European Data Privacy Law and Online Business* (Oxford University Press Oxford 2003)

Larremore 1912 *Columbia L Rev*

Larremore D "The Law of Privacy" 1912 *Columbia Law Review* 693-708

Lloyd *Information Technology Law*

Lloyd IJ *Information Technology Law* (Butterworths London 2004)

Madsen *Personal Data Protection*

Madsen W *Handbook of Personal Data Protection* (Macmillan Publishers London 1992)

McQuoid-Mason *Privacy*

McQuoid-Mason DJ *The Law of Privacy in South Africa* (Juta Cape Town 1978)

Mount 1992-1995 *Auckland University L Rev*

Mount S "The Privacy Act 1993" 1992-1995 *Auckland University Law Review* 408-413

Neethling 2007 *TSAR*

Neethling J “Die hoogste hof van appèl verleen erkenning aan die reg op identiteit as persoonlikheids- en fundamentele reg: regspraak” 2007 *Tydskrif vir Suid-Afrikaanse Reg* 834-838

Neethling 2002 *THRHR*

Neethling J “Aanspreeklikheid vir nuwe risiko’s: moontlikhede en beperkinge van die Suid-Afrikaanse deliktereg” 2002 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 574-592

Neethling 1980 *THRHR*

Neethling J “Die kredietburowese en databeskerming” 1980 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 141-155

Neethling “Databeskerming”

Neethling J “Databeskerming: Motivering en Riglyne vir Wetgewing in Suid-Afrika” in Strauss SA (ed) *Huldigingsbundel vir WA Joubert* (Butterworths Durban 1988)

Neethling *Privaatheid*

Neethling J *Die Reg op Privaatheid* (LLD-thesis Unisa 1976)

Neethling, Potgieter and Visser *Law of Delict*

Neethling J, Potgieter JM and Visser PJ *Law of Delict* (Butterworths Durban 2005)

Neethling, Potgieter and Visser *Law of Personality*

Neethling J, Potgieter JM and Visser PJ *Neethling’s Law of Personality* (Butterworths Durban 2005)

NZ Department of Justice White Paper

New Zealand Department of Justice A Bill of Rights for New Zealand: White Paper (Department of Justice Wellington 1985)

NZLC SP 19

New Zealand Law Commission Study Paper 19 *Privacy: Concepts and Issues: Review of the Law of Privacy*. Stage 1 (NZLC Wellington 2008)

OECD Guidelines

Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum* (OECD Paris 1981)

OECD Recommendation

Organisation for Economic Cooperation and Development *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Paris 1980)

Palmer 1975 NZLJ

Palmer G "Privacy and the Law" 1975 *New Zealand Law Journal* 747-756

Prosser 1960 Cal L Rev

Prosser WL "Privacy" 1960 (48) *California Law Review* 383-423

Rogers Torts

Rogers WVH *Winfield & Jolowicz on Torts* (Sweet and Maxwell London 1989)

Roos 2007 SALJ

Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African position" 2007 *South African Law Journal* 400-433

Roos 2006 CILSA

Roos A "Core Principles of Data Protection Law" 2006 *Comparative and International Law of South Africa* 102-130

Roos 1990 *TSAR*

Roos A "Data privacy: The American experience" 1990 *Tydskrif vir Suid-Afrikaanse Reg* 264-278

Roos *Data (Privacy) Protection*

Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD-thesis Unisa 2003)

Schulze 1994 *THRHR*

Schulze WG "The LOA life register – A snap survey of possible legal pitfalls" 1994 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 75-86

Shroff "Privacy and Sovereignty"

Shroff M (NZ Privacy Commissioner) "Privacy and Sovereignty: Data Fight or Flight?" An address to GOVIS 2007 – Innovation in ICT (Wellington 10 May 2007)

Tobin 2004 *TLJ*

Tobin R "Yes, Virginia, There is a Santa Claus: The Tort of Invasion of Privacy in New Zealand" 2004 (12) *Torts Law Journal* 95-107

Tobin 2000 *NZLJ*

Tobin R "Invasion of Privacy" 2000 *New Zealand Law Journal* 216-218, 222

Tobin "Privacy and Freedom of Expression"

Tobin R "Privacy and Freedom of Expression in New Zealand" in Colvin M (ed) *Developing Key Privacy Rights* (Hart Publishing Oxford 2002)

Turkington and Allen *Privacy Law*

Turkington RC and Allen A *Privacy Law: Cases and Materials* (West Group St Paul Minnesota 1999)

Warren and Brandeis 1890 *Harv L Rev* 193

Warren S and Brandeis L "The Right to Privacy" 1890 (4) *Harvard Law Review* 193-220

Westin Privacy and Freedom

Westin AF Privacy and freedom (Atheneum New York 1967)

Register of court cases

South Africa

Bernstein v Bester NO 1996 2 SA 751 (CC)

Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening) 2001 4 SA 938 (CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 2 SA 451 (A)

Gosschalk v Rossouw 1966 2 SA 476 (C)

Grutter v Lombard 2007 4 SA 89 (SCA)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2001 1 SA 545 (CC)

Janit v Motor Industry Fund Administrators (Pty) Ltd 1995 4 SA 293 (A)

Jansen van Vuuren v Kruger 1993 4 SA 842 (A)

Kidson v SA Associated Newspapers Ltd 1957 3 SA 461 (W)

La Grange v Schoeman 1980 1 SA 885 (E)

Mhlongo v Bailey 1958 1 SA 370 (C)

Motor Industry Fund v Janit 1994 3 SA 56 (W)

National Media Ltd v Jooste 1996 3 SA 262 (A)

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 3 SA 244 (C)

Protea Technology Ltd v Wainer [1997] 3 All SA 594 (W) 608

Rhodesian Printing and Publishing Co Ltd v Duggan 1975 1 SA 590 (R)

S v A 1971 2 SA 293 (T)

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 4 SA 376 (T)

386

New Zealand

Andrews v TVNZ [15 December 2006] HC AK CIV 2004-4-4-353

Auckland Medical Aid Trust v Taylor [1975] 1 NZLR 728 737 (CA)

Bradley v Wingnut Films [1993] 1 NZLR 415 (HC)

Brooker v Police [2007] NZSC 30
Hosking v Runting [2005] 1 NZLR 1 (CA)
L v G [2002] DCR 234, [2002] NZAR 495
Moulton v Police [1980] 1 NZLR 443 (CA)
P v D [2000] 2 NZLR 591 (HC)
R v Fraser [1997] 2 NZLR 442 (CA)
R v Grayson and Taylor [1997] 1 NZLR 399 (CA)
Ramsay v Cooke [1984] 2 NZLR 680 (HC)
Rogers v Television New Zealand Ltd [2007] NZSC 91
Savelio v R [2005] NZCA 198
Transport Ministry v Payn [1977] NZLR 50 64 (CA)
Tucker v News Media Ownership Ltd [1986] 2 NZLR 716 (HC)
TV3 Network Services Ltd v Farhey [1999] 2 NZLR 129 (CA)

United Kingdom

Campbell v MGN [2004] 2 AC 457 (HL)
Douglas v Hello! Ltd [2001] QB 967; [2001] 2 All ER 289
Kaye v Robertson [1991] FSR 62
Malone v Metropolitan Police Commissioner (No 2) [1979] 2 All ER 620
R (on the application of Wainwright) v Richmond upon Thames London Borough Council [2001] EWCA Civ 2062 CA
R v Brown [1996] AC 543 557 (HL)

Register of legislation

Bill of Rights Act 1990 (NZ)
Broadcasting Act 1976 (NZ)
Broadcasting Act 1989 (NZ)
Care of Children Act 2004 (NZ)
Children's Online Privacy Protection Act 1998 (USA)
Computer Matching and Privacy Protection Act 1988 (USA)
Constitution Act 1986 (NZ)
Constitution of the Republic of South Africa 1996 (SA)

Crimes Act 1961 (NZ)
Data Protection Act 1998 (UK)
Electronic Communications and Transactions Act 25 of 2002 (SA)
Electronic Communications Privacy Act 1986 (USA)
Fair Credit Reporting Act 1970 (USA)
Human Rights Act 1977 (NZ)
National Credit Act 34 of 2005 (SA)
Privacy Act 1974 (USA)
Privacy Act 1993 (NZ)
Privacy Commissioner Act 1991 (NZ)
Privacy Protection Act 1980 (USA)
Promotion of Access to Information Act 2 of 2000 (SA)
Right to Financial Privacy Act 1978 (USA)
Statute of Westminster Adoption Act 1947 (NZ)
Supreme Court Act 2003 (NZ)
Telecommunications Act 1996 (USA)
Wanganui Computer Centre Act 1976 (NZ)
Wet Bescherming Persoonsgegevens 2000 (Netherlands)

Register of international documents

Charter of Fundamental Rights of the European Union [2000] *Official Journal C*
364/1

Council of Europe Convention for the Protection of Individuals with Regard to
Automatic Processing of Personal Data No 108/1981 (Strasbourg 28 Jan
1981)

European Union Directive on the Protection of Individuals with regard to the
Processing of Personal Data and on the Free Movement of such Data
Directive 95/46/EC 1995 *Official Journal L* 281/ 31

Treaty of Waitangi 1840 (NZ)

Treaty on European Union 1992

United Nations International Covenant on Civil and Political Rights General
Assembly Resolution 2200A (XXI) 16 December 1966
107/184

Register of Internet sources

BSA <http://www.bsa.govt.nz> 24 Nov

BSA 2008 Information about the Broadcasting Standards Authority [Found on internet] <http://www.bsa.govt.nz> [Date of use 24 November 2008]

Council of Europe 2008 http://www.coe.int/T/e/Com/about_coe/ 16 Jun

Council of Europe 2008 About the Council of Europe [Found on internet] http://www.coe.int/T/e/Com/about_coe/ [Date of use 16 June 2008]

DoC *Safe Harbor Agreement* <http://www.export.gov/safeharbor> 24 Nov

Department of Commerce *Safe Harbor Agreement* [Found on internet] <http://www.export.gov/safeharbor> [Date of use 24 November 2008]

Engelbrecht 2008 <http://www.itweb.co.za/sections> 16 Jun

Engelbrecht L 20 February 2008 Data Privacy Bill in suspended animation [Found on internet] <http://www.itweb.co.za/sections> [Date of use 20 February 2008]

EU 2008 http://europa.eu/abc/index_en.htm 24 Nov

EU 2008 Countries [Found on internet] http://europa.eu/abc/index_en.htm [Date of use 24 November 2008]

Greville 2002 *LLRX* <http://www.llrx.com/> 16 Jun

Greville M "An introduction to New Zealand Law and Legal Information" 2002 *LLRX* [Found on internet] <http://www.llrx.com/features/newzealand.htm> [Date of use 16 June 2008]

NZ Privacy Commissioner Fact Sheet no 2 <http://www.privacy.org.nz> 18 Jun

NZ Privacy Commissioner Fact Sheet no 2: Information Privacy Principles [Found on internet] <http://www.privacy.org.nz> [Date of use 18 June 2008]

NZ Privacy Commissioner *Annual Report 2007* <http://www.privacy.org.nz/> 27

Nov

New Zealand Privacy Commissioner *Annual Report 2007* [Found on

internet] <http://www.privacy.org.nz/assets/Uploads/Annual-Report-of-the-Privacy-Commissioner-2007.pdf> [Date of use 27 November 2008]

OECD 2008 <http://www.oecd.org> 24 Nov

OECD 2008 Organisation for Co-operation and Development [Found on internet] <http://www.oecd.org> [Date of use 24 November 2008]

SALRC *Privacy and Data Protection* Discussion Paper 109

<http://www.doj.gov.za/salrc/> 24 Nov

South African Law Reform Commission *Privacy and Data Protection*

Project 124 Discussion Paper 109 [Found on internet]

<http://www.doj.gov.za/salrc/> [Date of use 24 November 2008]

List of abbreviations

ALI	American Law Institute
art	article(s)
BSA	Broadcasting Standards Authority
ch	chapter(s)
DoC	Department of Commerce
EC	European Community
EU	European Union
NZ	New Zealand
NZBORA	New Zealand Bill of Rights Act
NZLC	New Zealand Law Commission
OECD	Organisation for Co-operation and Development
par	paragraph(s)
reg	regulation(s)
s	section(s)
SALRC	South African Law Reform Commission
sch	schedule(s)
UK	United Kingdom
USA	United States of America