LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

Preliminary Paper 49

PROTECTING PERSONAL INFORMATION FROM DISCLOSURE

A discussion paper

The Law Commission welcomes your comments on this paper and seeks your response to the questions raised.

These should be forwarded to the Law Commission
PO Box 2590, DX SP 23534, Wellington
com@lawcom.govt.nz
by 30 April 2002

February 2002
Wellington, New Zealand

The Law Commission is an independent, publicly funded, central advisory body established by statute to undertake the systematic review, reform and development of the law of New Zealand. Its purpose is to help achieve law that is just, principled, and accessible, and that reflects the heritage and aspirations of the peoples of New Zealand.

The office of the Law Commission is at 89 The Terrace, Wellington
Postal address: PO Box 2590, Wellington 6001, New Zealand
Document Exchange Number: SP 23534
Telephone: (04) 473–3453, Facsimile: (04) 471–0959
Email: com@lawcom.govt.nz
Internet: www.lawcom.govt.nz

National Library of New Zealand Cataloguing-in-Publication Data
Protecting personal information from disclosure : a discussion paper.
(Preliminary paper (New Zealand. Law Commission)) ; 49.
ISBN: 1-877187-84-4
1. New Zealand. Privacy Act 1993. 2. Privacy, Right of—New Zealand.
I. New Zealand. Law Commission. II. Title. III. Series.
342.930858—dc 21

Use of submissions

The Law Commission's processes are essentially public, and it is subject to the Official Information Act 1982. Thus copies of submissions made to the Commission will normally be made available on request, and the Commission may mention submissions in its reports. Any request for the withholding of information on the grounds of confidentiality or for any other reason will be determined in accordance with the Official Information Act 1982.

Preliminary Paper/Law Commission, Wellington, 2002
ISSN 0113–2245 ISBN 1–877187–84–4
This preliminary paper may be cited as: NZLC PP49

This discussion paper is also available on the Internet at the Commission's website: http://www.lawcom.govt.nz

Contents

Preface

IN MANY AREAS of the law there is an underlying tension between the need to protect the rights of individual citizens and the need to benefit the community as a whole.

Nowhere is this tension more acute than in assessing the balance that must be struck between the natural desire of an individual to protect his or her privacy and the need of the community's elected representatives to obtain information to assist in making good policy decisions for the benefit of the community as a whole.[1]

This underlying tension also manifests itself when the desire for privacy is set against the need for freedom of expression within our society to be as unconstrained as possible and for information to be available within commercial markets so that participants can make informed decisions.

In the international context, there have been concerted efforts to harmonise domestic privacy laws to prevent privacy concerns inhibiting international trade and that too can require choices between competing values.

Particular challenges also result from the increased use of electronic commerce and the technological environment. We have already commented on these issues in the context of electronic commerce in *Electronic Commerce Part Two: A Basic Legal Framework* [ECom 2][2] and *Electronic Commerce Part Three: Remaining Issues* [ECom 3].[3] But we did not need to question the Privacy Act 1993 or its underlying philosophy in those papers.

The Privacy Act 1993 does not deal with all aspects of privacy. It governs the availability and protection of personal information, and it is that aspect of privacy which, under section 7(2) of the Law Commission Act 1985, our reference from the Minister Responsible for the Law Commission requests that we consider in these terms:

> As the first stage of a project to deal comprehensively with the legal protection of rights of privacy, to consider the legal protection of personal information, and in particular:
> - to define the proper objectives of any statutory regulation of the availability of personal information; and
> - to identify the statutory machinery necessary to attain such objectives; and

---

1 Noel Whitty, Therese Murphy and Stephen Livingstone *Liberties: The Human Rights Act Era* (Butterworths, London, 2001) 279. See chapter 6 for further discussion on the related point of how different conceptions of the relationship between the individual and society manifest in different perceptions of the value of privacy.

2 Law Commission *Electronic Commerce Part Two: A Basic Legal Framework: NZLC R58* (Wellington, 1999) ch 11.

3 Law Commission *Electronic Commerce Part Three: Remaining Issues: NZLC R68* (Wellington, 1999) ch 5.

- to consider the future role of the Privacy Act 1993 in its existing or any amended form.

The reference requires us to consider afresh the public policy objectives behind the Privacy Act 1993 and the statutory machinery necessary to achieve those objectives.

No review of the law takes place in a vacuum. Consequently, we must keep in mind the constraints already referred to and the need to strike a proper balance between the rights of individual citizens and the interests of the whole community. On the day that the Minister signed our reference, 11 September 2001, tragic events unfolded in the United States, which now raise questions about the proper balance between the protection of personal information and the need to enable information to be retrieved and used for law enforcement or national security purposes. It is essential that our discussion is dispassionate and not a reflex reaction to terrorism.

In this preliminary paper we:

- first, consider the principles underlying the Privacy Act 1993 and review the domestic and international imperatives that led Parliament to conclude that the Act was necessary and desirable when it was enacted;
- second, challenge the underlying assumptions to generate an informed debate on them. This is necessary because we are undertaking this review more than eight years after the enactment of the Act. We seek to provoke responses that will assist us in determining how to weigh competing public policy factors; and
- third, isolate the questions that must be addressed to answer the three questions raised by the reference. Those questions will be addressed fully once we have received public submissions. A summary of questions we pose is to be found at pages 28–29.

In preparing this paper, we have drawn on a review of the Act by the Privacy Commissioner, *Necessary and Desirable*,[4] and a scoping paper[5] prepared for the Associate Minister of Justice by Mai Chen of Chen Palmer & Partners, to whom we express our thanks.

We are anxious to receive a wide range of information and expressions of opinion on the questions raised in chapter 4 of this paper. Submissions should be made to the Law Commission on or before 30 April 2002. Submissions can be sent by email to com@lawcom.govt.nz. When sending email submissions, please use the words Protecting Personal Information in the subject line. The Commissioner to whom enquiries should be referred is Judge Patrick Keane, one of the Commissioners who has contributed to this paper. The researcher involved in this project was Kerry Davis to whom we express our appreciation.

---

[4] Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review: Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act* (Auckland, 1998).

[5] Mai Chen "Scoping Paper on the Privacy Act 1993" prepared for the Hon Margaret Wilson, Associate Minister of Justice (Chen Palmer & Partners, Wellington, 27 April 2001).

1
The existing statutory framework

WHAT IS PRIVACY?

1 AN ANTHROPOLOGIST is likely to describe "privacy" as a human being's need for protection against the intrusions of other human beings, both physical and by the imposition of social pressures.[6] A law reformer, concerned to try to find a definition sufficiently hard-edged to be usable in the formulation of a legal rule, faces greater difficulties.

2 The word "privacy" is not one to which the law ascribes a precisely defined meaning. It is not what lawyers call a "term of art". In its broadest sense, privacy embraces such concepts as:

- freedom from surveillance, whether by law enforcement or national security agents, stalkers, paparazzi or voyeurs;
- freedom from physical intrusion into one's body, through various types of searches or drug testing procedures, or into one's immediate surroundings;
- control of one's identity; and
- protection of personal information.

3 Our Terms of Reference do not require us to consider whether it is useful to characterise these concepts under the single heading "privacy" and what would be the precise tests of eligibility.

4 It is generally agreed that if a discrete set of legal rules for the law of privacy could be identified, they would include the various legal protections of personal information. This preliminary paper is concerned with the protection of personal information from disclosure.

5 It makes sense to deal with the availability of personal information separately from, and before considering, privacy in general. Privacy is an elusive concept, but the protection of personal information is capable of reasonably clear definition. One view expressed makes the point vividly that:

> By locating, as the core of the issue, the regulation of "personal information," the subject is liberated from a tendentiously predetermined general theory, and specific answers may more easily be sought to specific, and frequently disparate, questions. Such progress is possible only if the law eschews the ambiguity, the abstractions and the poverty of "privacy."[7]

---

6 Barrington Moore Jr *Privacy: Studies in Social and Cultural History* (ME Sharpe Inc, Armonk NY, 1984) 72.

7 Raymond Wacks "The Poverty of Privacy" in Raymond Wacks (ed) *Privacy* (Dartmouth Publishing Company, Aldershot, 1993) vol 1, 197.

6 The Privacy Act 1993 is basically concerned with personal information, despite the apparently wide subject matter conveyed by its title.[8] The Long Title to the Act records that it is:

> An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular,—
>
> (a) To establish certain principles with respect to—
> (i) The collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
> (ii) Access by each individual to information relating to that individual and held by public and private sector agencies; and
>
> (b) To provide for the appointment of a Privacy Commissioner to investigate complaints about interferences with individual privacy; and
>
> (c) To provide for matters incidental thereto.

THE ORIGIN OF THE PRIVACY ACT 1993

7 In his 1998 review, the Privacy Commissioner described the backdrop to the enactment of the Privacy Act 1993 in the following terms:

> Privacy has been a significant national and international concern for over 30 years. During the 1960s and 1970s a range of concerns about the relationship between citizen and state emerged with the perceived growing threat of large computer databanks. The 1980s saw significant efforts at international privacy standard setting and legislative efforts to provide adequate protection to privacy with 1984 a favourite time for reflection on technological challenges to individual privacy. The 1990s have seen technological advances undreamed of by George Orwell with the worldwide linking of computers, the electronic tracking of consumers and citizens and advances from the microscopic work of the Human Genome Project through to global satellite surveillance from outer space.
>
> Together with the unease at entering a "brave new world" there remain a host of routine, but hugely important, privacy issues in everyday lives. Issues revolving around the information held on personnel files. The maintenance of blacklists in employment and housing. The accuracy of information upon which credit decisions are made. The wish to have our homes secure from unwanted intrusions.
>
> It is in this environment that the Privacy Act 1993 was enacted. The Act covers a variety of matters as will be apparent from reading this report. Two central features are the establishment of a Privacy Commissioner and a set of information privacy principles. The Privacy Commissioner is an independent official. . . . The information privacy principles apply to all agencies in the public and private sectors and govern the collection, holding, use and disclosure of personal information. Individuals have certain entitlements under the Act including to access and seek correction of personal information held by agencies and to obtain redress for interferences with their privacy.[9]

---

[8] The change of name from the "Privacy of Information Bill" was proposed by the Privacy Commissioner and agreed to despite the opposition of the Secretary for Justice. The Secretary opposed the name "Privacy Act" based on the fact that it was inaccurate, because the statute did not comprehensively deal with privacy. Indeed the title of the Act is potentially misleading, as it implies a broad protection of privacy but actually prescribes a disclosure regime that only relates to one particular aspect of privacy – personal information.

[9] Office of the Privacy Commissioner, above n 4, 1.

8 Legislation and policy touched on the question of privacy during the 1970s and 1980s:[10]

- Section 24(1)(g) of the Broadcasting Act 1976 required broadcasters to consider the privacy of individuals.[11]
- The Wanganui Computer Centre Act 1976 addressed the availability of personal information retained on a national law enforcement database. A special Privacy Commissioner was established[12] and empowered to investigate complaints about the inaccuracy, omission and unauthorised collection of information about a person on the computer system.[13]
- Part V of the Human Rights Commission Act 1977 conferred functions on the Human Rights Commission that required it to examine and advise on protecting the privacy of individuals.
- In 1984, the Human Rights Commission published a discussion paper, which set out the then legal position with regard to privacy generally.[14]
- In 1987, the then Department of Justice published *Data Privacy: An Options Paper*.[15]

9 On 5 August 1991, the National Government introduced a Privacy of Information Bill as a consequence of its first budget. There was resistance to applying the proposed legislative regime to the private sector, and the Select Committee to which the bill as amended was referred did not report the Bill back until 18 March 1993. It came into force as the Privacy Act 1993 on 1 July that year. It is clear from the third reading speeches that the compilation of data made possible by new technology justified the legislation in the minds of members on both sides of the House.[16]

AN OVERVIEW OF THE PRIVACY ACT 1993

10 There is no general definition in the Privacy Act 1993 of "personal information" beyond "information about an identifiable individual".[17] The word "individual" is defined as a natural person and therefore excludes companies and other corporations.[18] The word "agency" is defined to mean any person or body of

---

[10] In international law, exhortations to protect "privacy" can be found in the earlier provisions of Article 12 of the Universal Declaration of Human Rights (UN General Assembly, 10 December 1948) and the very similar provisions of Article 17 of the International Covenant on Civil and Political Rights (UN General Assembly, 16 December 1966).

[11] See *TV3 Network Services Limited v Broadcasting Standards Authority* [1995] 2 NZLR 720, 727. Eichelbaum CJ referred to that provision as a forerunner to s 4(1)(c) of the Broadcasting Act 1989 with which His Honour was concerned.

[12] Section 5 of the now repealed Wanganui Computer Centre Act 1976.

[13] Sections 9 and 15 of the now repealed Wanganui Computer Centre Act 1976.

[14] Tim McBride *Privacy Review: A Discussion and Resource Paper Prepared for and in Consultation with the Human Rights Commission* (Human Rights Commission, Auckland, 1984).

[15] Tim McBride *Data Privacy: An Options Paper* (Government Printer, Wellington, 1987, released by the Minister of Justice the Rt Hon Geoffrey Palmer).

[16] (5 May 1993) 535 NZPD 15209–15213.

[17] Privacy Act 1993, s 2(1).

[18] Privacy Act 1993, s 2(1).

persons, incorporated or not, and includes the public and private sectors.[19] The Act does not apply to the Governor General, members of parliament, ombudsmen, news organisations, commissions of inquiry, courts and tribunals, and a few other miscellaneous bodies.[20] The keys to the statute are the 12 Information Privacy Principles set out in section 6, which are annexed to this paper as Appendix A.

11 The principles must be read in their entirety, because they contain a number of qualifications.[21] However, the following is a summary of those principles.

Principle 1: The purpose for obtaining the information must be lawful and connected with a function of the agency. The collection of the information must be necessary to that function.

This principle limits the information that can be collected to what is necessary for an agency to achieve its lawful purpose and prevents the collection of information that is unnecessary or excessive.[22]

Principle 2: An agency must collect personal information directly from the individual concerned, unless the circumstances are within one of the exceptions set out in principle 2(2).

Principle 3: The person concerned should be informed:
- that the information is being collected;
- of the reason that the information is being collected;
- of whom the intended recipients of the information are and their contact details;
- of the law that authorises the collection of information;
- of whether the supply of the information is voluntary or mandatory;
- of the consequences of not providing the information; and
- that they have the right to have access to, and to correct, personal information about themselves.

This process must be undertaken before the information is collected or as soon as possible after it has been collected.[23]

However, an agency is not required to comply with the process outlined above if it has done so once already,[24] or if the circumstances come within one of the exceptions set out in principle 3(4).

Principle 4: Personal information cannot be collected by unlawful, unfair or unreasonably intrusive means.

---

19 Privacy Act 1993, s 2(1)(a).

20 Privacy Act 1993, s 2(1)(b).

21 Principles are characteristically short and clearly expressed. The extensive qualification of the principles in section 6 of the Act, arguably, hinders their comprehension. As an example of a principle that relates to a privacy issue which is expressed succinctly see principle 10 from the New Zealand Medical Association's Code of Ethics:

> Keep in confidence information derived from a patient, or from a colleague regarding a patient, and divulge it only with the permission of the patient except when the law requires otherwise.

22 Office of the Privacy Commission, above n 4, 61, para 2.3.6.

23 Privacy Act 1993, s 6, principle 3(2).

24 Privacy Act 1993, s 6, principle 3(3).

Principle 5: An agency that holds personal information must store it securely to prevent any loss of, unauthorised access to, use, modification, disclosure, or any other misuse of it.

Principle 6: An individual is entitled to confirmation from an agency that it holds personal information on him or her and to have access to it, provided the agency can retrieve it readily.

Principle 7: An individual is entitled to request that an agency correct personal information that it holds about them. If the correction is not made, they are entitled to have a statement attached to the information that the correction was sought but not made.[25]

Principle 8: An agency that holds personal information must ensure, before using it, that it is accurate, up to date, complete, relevant and not misleading.

Principle 9: An agency that holds personal information must not keep it any longer than required for lawful purposes.

Principle 10: An agency cannot use information for any purpose other than the one that it was obtained for, unless it comes within one of the exceptions set out in principle 10(a)–(g).

Principle 11: An agency that holds personal information must not disclose it unless the circumstances come within one of the exceptions set out in principle 11(a)–(h).

Principle 12: An agency must not assign a unique identifier to an individual unless it is required for the efficient performance of its functions.

An agency must not assign an identifier that it knows has been assigned to that individual by another agency, unless those two agencies are associated persons under the Income Tax Act 1994.[26]

An agency that assigns unique identifiers must ensure that the individual's identity is clearly established.

An agency cannot require an individual to disclose any identifier assigned to them, unless it is, or is directly related to, one of the purposes for which it was assigned.

12 In the present Privacy Commissioner's words:

> Limiting use and disclosure of personal information other than for purposes specified at the time of collection (or compatible purposes or those authorised by the individual concerned or by law) lies at the heart of any data protection law.[27]

The right of individuals to correct misinformation about them held by an agency is also a central ingredient of privacy law.[28]

---

[25] Office of the Privacy Commissioner, above n 4, 75, para 2.9.1.

[26] Income Tax Act 1994, s OD 7.

[27] Office of the Privacy Commissioner, above n 4, 84, para 2.12.1. See principles 10 and 11.

[28] See principles 6 and 7.

13 The Privacy Act also contains a list of materially similar, but not identical, exceptions.[29] In particular, the exceptions allow for non-compliance when an agency believes that:

- the information is publicly available;
- the individual concerned would authorise the non-compliance;
- it would not prejudice the interests of the individual concerned;
- compliance would prejudice the purposes of the collection;
- compliance is not practical;
- the information will not be used in a form that identifies the individual concerned, including statistical or research purposes; and
- collection of the information is authorised under section 54 of the Act.

14 There are also a number of countervailing public interests that prevail over compliance with the principles. In particular, non-compliance may be necessary:

- to ensure that any public sector agency's efforts to prevent, detect, investigate, prosecute and punish offences are not hindered;
- for the enforcement of a law imposing a pecuniary penalty or the protection of public revenue; or
- for the conduct of proceedings before a court.

15 Section 54 allows the Commissioner to authorise what would otherwise be a breach of some principles.[30] The Commissioner must first be satisfied that there are special circumstances, such as a countervailing public interest or a clear benefit to the individual, that outweigh any interference with the individual's privacy.[31] In practice "few applications under section 54 have been received".[32]

16 Where a significant breach of an information privacy principle occurs, the individual concerned can seek a remedy by complaining to the Privacy Commissioner.[33]

17 If the Commissioner considers that the complaint, or any part of it, relates to a matter within the jurisdiction of the Ombudsman or the Health and Disability Commissioner, it must be referred to and dealt with by the appropriate office. Section 72B also provides for matters within the jurisdiction of the Inspector-General of Intelligence and Security to be dealt with by the Inspector-General. The complainant must be advised that her or his complaint has been referred to another office.[34]

18 The Commissioner must investigate, conciliate and attempt to secure a settlement. If a settlement cannot be secured, the Commissioner must refer the matter to the Director of Human Rights Proceedings to determine whether proceedings should be taken before the Human Rights Review Tribunal.[35] If the Director of Human Rights

---

29 Office of the Privacy Commissioner, above n 4, 62, para 2.4.6. See principles 2, 3, 10 and 11.

30 See principles 2, 10 and 11.

31 Office of the Privacy Commissioner, above n 4, 219, para 6.10.2.

32 Office of the Privacy Commissioner, above n 4, 219, para 6.10.3.

33 Privacy Act 1993, s 66.

34 Privacy Act 1993, ss 72(3), 72A(3) and 72B(3).

35 Privacy Act 1993, s 77.

Proceedings decides that the matter warrants it, proceedings must be instituted, on behalf of either an individual or a class, before the Human Rights Review Tribunal.[36] The Tribunal, in turn, may grant one or more of the following remedies:[37]

- a declaration that the action constituted an interference with the individual's privacy;
- an order restraining the defendant from continuing or repeating the interference;
- damages for pecuniary loss, loss of any benefit, and humiliation, loss of dignity and injury to feelings;[38] and
- an order that the defendant perform any acts specified to remedy the interference or redress any loss or damage.

19 If the Director of Human Rights Proceedings decides that the matter does not have substance and declines to refer it to the Human Rights Review Tribunal, the aggrieved complainant may herself or himself bring proceedings before the Tribunal.[39]

---

[36] Privacy Act 1993, s 82.

[37] Privacy Act 1993, s 85.

[38] Privacy Act 1993, s 88(1)(a)–(c).

[39] Privacy Act 1993, s 83.

2
The international context

INTERNATIONAL HARMONISATION

20 In ECom 3 we discussed the steps that have been taken internationally to harmonise privacy and data protection law. In paragraphs 52–59 of ECom 3 we said:

> 52 The privacy laws of different jurisdictions vary considerably. As noted above, the European Union has very strict data protection laws. The United States, in contrast, has predominantly relied on self-regulation.
>
> 53 Attempts have been, and are being, made at an international level to achieve a harmonious approach to privacy law. The impetus for this movement is the recognition that privacy is an important trade issue, as data privacy concerns can create a barrier to international trade. Because of this, the General Agreement on Trade in Services, for example, contains a term stating that the Agreement does not prevent member states from adopting measures necessary to secure "the protection of the privacy of individual records and accounts".[40]
>
> 54 In 1980 the Organisation for Economic Cooperation and Development (OECD) released the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, perhaps the most significant attempt at international harmonisation. The Guidelines were intended to provide a common framework for national privacy laws, in order to ensure that privacy concerns do not impose a barrier to international trade. The Guidelines establish technologically neutral principles for the collection, retention and use of personal information. The OECD's work in this area is ongoing. In 1998 it held a Conference on Electronic Commerce, which issued a Declaration reaffirming the objectives set out in the 1980 Guidelines. In December 1999 the OECD released its Consumer Protection Guidelines for E-Commerce, which also recommended compliance with the 1980 OECD privacy principles.
>
> 55 The OECD has created a Privacy Statement Generator to help implement the 1980 Guidelines in the electronic world. The Generator is intended to offer guidance on compliance with the Guidelines and to help organisations develop privacy policies and statements for display on their websites. The Generator uses a questionnaire to gather information about an organisation's personal data practices. The answers are then fed into a preformatted draft policy statement. The draft statement will provide an indication of the extent to which an organisation's privacy practices are consistent with the OECD Privacy Guidelines. The Generator offers links to private sector organisations with expertise on developing privacy policies, and to government agencies, non-governmental organisations and private bodies that give information on

[40] Article XIV(c)(ii), Part II, General Agreement on Trade in Services.

applicable regulations. The Generator has been endorsed by the OECD's 29 member countries and is available free of charge.[41]

56 Other international agreements aimed at harmonising approaches to data privacy tend to resemble or reflect the OECD Guidelines. These include the United Nations Guidelines for the Regulation of Computerised Personal Data Files,[42] the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[43] and the EU Privacy Directive.[44] These agreements typically contain provisions permitting cross-border data flow to countries with similar levels of data protection.

57 There are also numerous international conferences and discussion forums which play an important role in contributing to international harmonisation through information exchange, education, and the development of instruments for privacy protection. These include annual international conferences of data protection commissioners, conferences of EU data protection commissioners, the International Working Group on Data Protection in Telecommunications, the International Organisation for Standardisation,[45] and the International Chamber of Commerce.

58 On another level, mechanisms have been developed to implement and enforce privacy principles on global networks. These include the development of means whereby consumers may use the internet anonymously (for example, the use of anonymous payment systems and digital certificates to avoid the

---

41 The Generator may be found at <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>.

42 United Nations High Commission for Human Rights Guidelines for the Regulation of Computerised Personal Data Files (Resolution 45/95 of 14 December 1990) were adopted by the UN General Assembly pursuant to article 10 of the UN Charter. The UN Guidelines apply to computerised personal data files (both public and private) and may be extended to manual files and to files on legal persons. Part A of the Guidelines are intended as the minimum privacy guarantees that should be provided in national legislation, and broadly reflect the basic principles in the OECD Guidelines. In addition, the UN Guidelines restrict the compilation of "sensitive data" within the principle of non-discrimination. United Nations members must take the United Nations Guidelines into account when implementing national regulations concerning computerised personal data files, but the procedures for implementing those regulations are left to the initiative of each State.

43 The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data asserts basic data privacy principles that are similar to those in the OECD Guidelines. However, it also includes a principle requiring appropriate safeguards for special categories of data (sensitive data) that reveal racial origin, political opinions or religious or other beliefs, that concern health or sexual life, or that relate to criminal convictions (article 6). The Convention is open to the accession of any State, whether a member of the Council of Europe or not.

44 The information privacy principles of the EU Directive are framed in terms of processing personal data but are in general terms similar to the information privacy principles found in the OECD Guidelines and the Council of Europe Convention. In several respects the principles of the Directive offer greater protection to data privacy. The EU Directive is likely to prove hugely influential outside the EU because of the data flow controls that it instigates.

45 The ISO Ad Hoc Advisory Group on Privacy undertook a study to examine whether there is a need, under the pressure of technological advances in global information structures, for an international standard to address information privacy, measure privacy protection and ensure global harmonisation. In June 1988 the Advisory Group concluded that it was premature to reach a determination on the desirability and practicality of ISO undertaking the development of international standards relevant to the protection of personal privacy.

need for personal data disclosure), the development of software that enables the user to control the use of cookies, the creation of industry standards and the certification of adequate privacy practices by trusted third parties.

59 New Zealand is highly dependent on its ability to trade internationally. For the last 16 years our governments have shown a commitment to reducing barriers to international trade. The international harmonisation of privacy and data protection law is an important factor in achieving that goal. We recommend continued involvement by New Zealand in these international forums.

21 This trend towards the international harmonisation of privacy law has implications for the domestic reform of privacy law. The rationale behind the harmonisation of privacy law, and the initiatives aimed at achieving harmonisation, raise, at least, the following questions:

- If the Privacy Act were to be modified or repealed, would it affect New Zealand's international relations or international trade?
- What, if any, adverse consequences may flow from inconsistencies between our domestic and the international privacy law?
- To what extent should the European Union Directive and its requirement for "adequate" privacy laws be taken into account?
- Does the possibility that the OECD guidelines may be departed from need to be considered?

OVERSEAS COMPARISONS

22 There are various privacy regimes around the world. In this paper we confine ourselves to three useful comparisons: Australia, Canada and the United Kingdom.

Australia

23 The Privacy Act 1988 (Commonwealth) is the primary domestic legislation on information privacy protection in Australia. It subjects federal government agencies to 11 Information Privacy Principles based on those in the OECD guidelines.[46] The Information Privacy Principles provide rights applicable throughout the lifecycle of information held by organisations from the time it is collected to its ultimate destruction.[47]

24 This Act was recently extended by the Privacy Amendment (Private Sector) Act 2000 (Commonwealth) to cover private sector organisations.[48] The amended Act began operating in December 2001 and introduced a set of National Privacy Principles to guide the way that private sector organisations deal with personal information.[49] It confers, on individuals, enforceable rights concerning their "personal information" against public and private sector organisations.[50]

---

[46] Privacy Act 1988 (Cth), s 14.

[47] Victorian Law Reform Commission *Privacy Law: Options for Reform: Information Paper* (Melbourne, 2001) 23.

[48] Victorian Law Reform Commission, above n 47, 23, para 4.9.

[49] To date, the private sector has only been subject to privacy obligations for the treatment of tax file numbers and credit reporting activities that involved the flow of personal information from one organisation to another.

[50] As defined in section 6(1) of the Privacy Amendment (Private Sector) Act 2000 (Cth).

25 A minimum standard of privacy protection is established under the later Act, but this can be substituted by approved industry codes.[51] The industry codes must meet at least the minimum standards in the National Privacy Principles.[52] The federal Freedom of Information Act 1982 also provides individuals with the right to access government records and correct personal information about themselves.[53]

26 All of the States and the Australian Capital Territory (but not the Northern Territory) also have freedom of information laws.[54]

27 Miscellaneous statutes also contain privacy-related measures. The Telecommunications Act 1979 (Commonwealth) regulates the interception of telecommunications. The Crimes Act 1914 (Commonwealth) contains a variety of privacy-related measures including offences relating to unauthorised:

- access to computers;[55]
- interception of mail and telecommunications;[56] and
- disclosure of Commonwealth government information.[57]

Canada

28 Canada has privacy legislation at the federal and provincial level covering government bodies.[58] The Privacy Act 1985 regulates the confidentiality, collection, correction, disclosure, retention and use of personal information by the federal public sector.[59]

---

[51] Privacy Amendment (Private Sector) Act 2000 (Cth), part 111AA.

[52] See section 18BB(2)(a) of the Privacy Amendment (Private Sector) Act 2000 (Cth). It is noteworthy that the National Principles impose a lower standard of protection in several areas than the EU Directive provides. For example, organisations are only required to obtain consent from customers for secondary use of their personal information for marketing purposes where this is "practicable". Otherwise, an organisation can initiate direct marketing contact provided that they give the individuals the choice to opt out of further communications. Controls on the transfer of personal information overseas are also limited. Organisations are only required to take "reasonable steps" to ensure personal information will be protected or to "reasonably believe" that the information will be subject to similar protection as Australian law applies.

[53] Freedom of Information Act 1982 (Cth), ss 11 and 48.

[54] The Victorian Law Reform Commission detailed State privacy laws in its recent paper *Privacy Law: Options for Reform,* above n 47. Paragraph 4.9 reads:

> In Victoria, the *Information Privacy Act 2000* was recently passed and comes into force in September 2001. It covers State Government agencies and private contractors to State Government. Similar public sector privacy legislation was also passed in New South Wales in 1998 and is being considered in other jurisdictions.

See the Privacy and Personal Information Protection Act 1998 (NSW). The Northern Territory intends to introduce public sector privacy legislation to complement the Commonwealth regime: Ministerial Statement of the Chief Minister of the Northern Territory, the Hon Denis Burke MLA *Northern Territory Hansard* 22 April 1999, available at <http://notes.nt.gov.au/lant/hansard/HANSARD8.NSF?OpenDatabase>, cited in Victorian Law Reform Commission, above n 47, 23.

[55] Crimes Act 1914 (Cth), s 76B.

[56] Crimes Act 1914 (Cth), parts VIIA and VIIB.

[57] Crimes Act 1914 (Cth), part VI, s 70.

[58] See the Privacy Commissioner of Canada website <http://infoweb.magi.com/~privcan/other.html>.

[59] Privacy Act RSC 1985, c P-21, ss 4–9.

29 Individuals also have the right to access and correct personal information about themselves held by federal government organisations.[60] The federal Access to Information Act 1985 complements and extends the Privacy Act by giving Canadians, and other individuals and corporations present in Canada, the right to apply for and obtain copies of federal government "records".[61]

30 In April 2000, the Personal Information Protection and Electronic Documents Act was approved by the federal Parliament.[62] The Act covers "organisations"[63] that process personal information "in the course of a commercial activity" and federally regulated employers with respect to their employees.[64] Organisations must comply with a national standard for the protection of personal information,[65] which is set out as principles in schedule 1 of the Act.[66]

31 However, the vast majority of information collected by the private sector is at the provincial level and is not currently protected by any provincial laws.

32 Miscellaneous statutes also contain a range of other privacy-related measures.[67] Most provinces also have some form of legislation protecting consumer credit information.

---

60 Privacy Act RSC 1985, c P-21, s 12.

61 The Access to Information Act RSC 1985, c A-1, s 4. This includes letters, memos, reports, photographs, films, microforms, plans, drawings, diagrams, maps, sound and video recordings, and machine-readable or computer files.

62 See the Privacy International website <http://www.privacyinternational.org/survey/index.html> for a comprehensive survey of the coverage of privacy and data protection laws around the world.

63 "Organisation" is defined as an association, a partnership, a person and a trade union.

64 Personal Information Protection and Electronic Documents Act 2000, c 5, s 4. The law took effect for federally regulated companies, such as banks, telecommunications enterprises, transportation and other businesses that trade data interprovincially and internationally, in January 2001. Medical records are exempted from the new law until 2002, and provincially regulated sectors are not covered for three years and only then if the province does not enact "substantially similar" laws.

65 Under section 2 "personal information" means information about an identifiable individual.

66 Personal Information Protection and Electronic Documents Act 2000, c 5, s 5. The Ontario Ministry of Consumer and Business Services detailed this principle-based approach to privacy:

> The principles in the . . . [Federal] legislation are based on the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.
>
> The CSA Code relects a broad consensus among businesses, consumer organizations and governments. It has been adopted as a voluntary national standard and is also enshrined in the federal privacy law.

Ontario Ministry of Consumer and Business Services *A Guide to Ontario's Consultation on Privacy Protection*, available at <http://www.cbs.gov.on.ca/mcbs/english/pdf/56HLLL.pdf>, 4.

67 Part VI of Canada's Criminal Code makes the unlawful interception of private communications a criminal offence: Criminal Code RS 1985 c C-46, ss 184, 184.5, 193, and 193.1.

The Telecommunications Act has provisions to protect the privacy of individuals, including the regulation of unsolicited communications under the Telecommunications Act 1993 c 38, ss 39 and 41.

The Bank Act, the Insurance Companies Act, and Trust and Loan Companies Act permit regulations to be made governing the use of information provided by customers under the Bank Act 1991 (Fed) c 46, ss 242, 244, and 459, the Insurance Companies Act 1991 (Fed) c 47, ss 489 and 607 and the Trust and Loan Companies Act 1991 (Fed) c 45, s 444, respectively.

United Kingdom

33 In the United Kingdom, the Data Protection Act 1998 implements the European Union Data Protection Directive. The Act requires data controllers to comply with a set of data protection principles about the personal data they process.[68] The following rights for data subjects are established in the Act:

- the right of access to personal data;[69]
- the right to prevent processing likely to cause unwarranted damage or distress;[70]
- the right to prevent processing for purposes of direct marketing;[71]
- rights in relation to automated decision taking;[72]
- the right to compensation for data controller failure to comply with certain requirements;[73] and
- rights in relation to rectification, blocking, erasure and destruction of inaccurate data.[74]

34 Principle 8 provides that personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.[75]

NEW ZEALAND'S PRIVACY LAW IN PERSPECTIVE

35 The Privacy Commissioner put New Zealand privacy law in perspective when he stated at the recent LawAsia Conference that:

> New Zealand is generally thought to have the most comprehensive national privacy law outside Europe.[76]

There are also sectoral laws for pensions, video surveillance, immigration, and Social Security under the Canada Pension Plan RSC 1985 c C-8, s 104.07, Criminal Code RS 1985 c C-46, s 487.01, Immigration Act SC 1985 c I-2, s 110, and Old Age Security Act RS 1985 c O-9, s 33.01, respectively.

The Young Offenders Act RS 1985 c Y-1, s 38 regulates what information can be disclosed about offenders under the age of 18, while the Corrections and Conditional Release Act 1992 c 20, ss 26 and 142 speaks to what information can be disclosed to victims and victims' families.

68 Data Protection Act 1998 (UK), s 4.

69 Data Protection Act 1998 (UK), ss 7–9.

70 Data Protection Act 1998 (UK), s 10.

71 Data Protection Act 1998 (UK), s 11.

72 Data Protection Act 1998 (UK), s 12.

73 Data Protection Act 1998 (UK), s 13.

74 Data Protection Act 1998 (UK), s 14.

75 See Data Protection Act 1998 (UK), schedule 1. The European Economic Area includes 15 European Union nations plus Iceland, Liechtenstein and Norway.

76 Bruce Slane "New Zealand's Privacy Law in Perspective" (speech to 17th Biennial LawAsia Conference, Christchurch, 4–8 October 2001).

36 Australian privacy law, for example, did not extend to the private sector at the time that our Privacy Act was introduced; and recent Australian privacy legislation, which applies to the private sector, has been criticised by the European Union for containing broad exceptions that significantly negate its effect.[77] It is estimated that 94 per cent of Australian businesses are excluded from its application.[78]

37 Similarly, Canada did not set out the ground rules for how private sector organisations may deal with personal information until 2001, and as indicated the coverage is limited. Canadian privacy legislation does not protect personal information collected by the private sector at the provincial level, which is where the majority of personal information is collected by the private sector.[79]

38 The issue is how comprehensive does New Zealand's legislation need to be? A related question is of practical importance: how comprehensive *can* it be?

---

[77] European Commission, Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs concerning its inquiry into the Privacy Amendment (Private Sector) Bill 2000 cited in Slane, above n 76.

[78] House of Representatives Standing Committee on Legal and Constitutional Affairs, "Advisory Report on the Privacy Amendment (Private Sector) Bill 2000", June 2000, para 2.20, cited in Slane above n 76. This is because the law does not apply to businesses with a turnover under $3 million. All employee data is also excluded from the Act.

[79] Privacy Commissioner of Canada, "Privacy Legislation in Canada", <http://www.privcom.gc.ca/fs-fi/fs2001-02_e.asp>.

3
Challenging the assumptions underlying the Privacy Act 1993

SNAPSHOTS

39 A 1999 *ECONOMIST* EDITORIAL DISCUSSING PRIVACY observed that:

> To earlier generations, escaping the claustrophobic all-knowingness of a village for the relative anonymity of the city was one of the more liberating aspects of modern life. But the era of urban anonymity already looks like a mere historical interlude. There is, however, one difference between past and future. In a village, everybody knew everybody else's business. In the future, nobody will know for certain who knows what about them. That will be uncomfortable. But the best advice may be: get used to it.[80]

40 A lawyer specialising in Internet issues recently wrote in *Newsweek* that:

> At the beginning of the last century, my grandparents sailed to America, leaving behind their Irish farming village. The people in their community knew my family's history, their opinions and personalities, friendships and feuds. At the beginning of this century, we are in some ways returning to that village. . . . We are, once again, becoming a transparent society – one where everyone knows everything about everyone else in real time. . . . Too often the privacy debate has been polarized between those who wish to fully prohibit the use of personal information and those who wish to fully exploit it. Most of us have a foot in both camps: we welcome the marvellous benefits of information technology, but we have an equally powerful desire for personal privacy. Perhaps the most that can be hoped for is a modus vivendi not unlike that reached in my grandparents' village. They may have chafed sometimes at their lack of privacy, but it gave them a sense of belonging to a larger community – as long as it was not abused. Common sense, in the end, prevailed. That is what we should aim for today as well.[81]

CHANGING VALUES WITHIN SOCIETY

41 "Since societies differ, the desire or need for privacy will vary historically, from one society to another and among different groups in the same society".[82] The belief that one benefits from being able to stop others from learning everyday personal facts about oneself is a very recent development in the history of Western ideas.

---

[80] "The End of Privacy" (1 May 1999) *The Economist* New York, 11.

[81] Christine Varney "The Death of Privacy?" (December 2000–February 2001) *Newsweek Special Edition* New York, 78–79.

[82] Moore, above n 6, 73.

42 The belief that the law should assist individuals to control the dissemination of personal information about them is even more recent than the desire for privacy.

43 In small communities, keeping personal information private is a practical impossibility. Few secrets can be kept from neighbours in small communities, but the impersonality of large communities makes privacy possible.

44 There have always been both societal and market restraints against the unauthorised disclosure of personal information. A gossip ceases to be the recipient of confidences. Customers are unlikely to be attracted to a business that gives out personal information about them. For example, a pharmacist who advises a customer of medication being taken by another customer may lose their business.

45 As recently as a decade ago, privacy law was still in an undeveloped state. Consequently, until the passing of the Privacy Act in 1993, a number of piecemeal legal measures protected the availability of personal information including:

- the rules governing various occupational groups, such as, lawyers, doctors and priests, which required non-disclosure and were legally enforceable;
- an implied duty of confidence in certain types of relationships;[83]
- a defamation claim;[84]
- parties to contracts of service contracting out of revelations of confidential matters;
- the confidentiality of information disclosed to State agencies under legal compulsion;[85] and
- a judge-made tort of privacy.

46 The public belief that the law should control the dissemination of personal information is attributable to two separate causes: firstly, the development of a mass audience media and the adoption by some media of a style that is generally seen as being unduly intrusive; and secondly, the public awareness of the ease with which personal information can be stored, sorted and retrieved with the aid of computers.

47 In paragraphs 165 and 166 of ECom 2, we noted views expressed in 1998 and 1999 respectively by Hon Justice Michael Kirby of the High Court of Australia and the current Privacy Commissioner on this topic. In those paragraphs we said:

> The speed, power, accessibility and storage capacity for personal information identifying an individual are now greatly increased. Some of the chief protections for privacy in the past arose from the sheer costs of retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming that its existence was known). Other protections for privacy arose from the incompatibility of collections with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy

---

[83] In *Duchess of Argyll v Duke of Argyll* [1967] Ch 302, the Court restrained the newspaper publication by a husband of marital confidences.

[84] In *Ettinghausen v Australian Consolidated Press Ltd* (1991) 23 NSWLR 443, the publication without consent of a photograph of a footballer that revealed his penis was the basis for a defamation action. Similarly, in *Kirk v AH & AW Reed* [1968] NZLR 801, the publication without consent of a photograph of "a reveller with his Christmas beer supply" supported a defamation action.

[85] See Tax Administration Act 1994, part 4 and subs 6(1) and 6(2)(c) and (e); Statistics Act 1975, s 37.

> largely disappear in the digital age. A vast amount of data, identified to a particular individual, can now be collated by the determined investigator. The individual then assumes a virtual existence which lives in cyberspace instead of in what is sometimes described as "meat space". The individual takes on a digital persona made up of a collection of otherwise unconnected and previously unconnectable data.[86]
>
> It is interesting to consider why, in a consumer age where quality, choice and convenience is demanded, the level of e-commerce is so low. One reason is the appeal of conventional shopping. Another is a lack of consumer confidence in doing business electronically . . . They worry about the security of their personal information and fear it may be misused.[87]

48 The modern literature on privacy is replete with expressions of concern at the capacity of computers to store and match information. Computerisation can repair those State organisational inefficiencies that have constituted the best defences against totalitarian excess in the past. Professor David Feldman asserts that:

> In the electronic age, those who control information about my health, wealth, ambitions and weaknesses can manipulate, if not control, my life.[88]

49 Sentiments of this sort led to the enactment of the Data Protection Act 1984 in the United Kingdom, which was confined in its effect to holding and processing information using computers.[89] This same fear of computerisation is reflected in the New Zealand statute,[90] and the literature includes accounts of the harm that can be done by those who gain unauthorised access to electronically stored information.[91]

50 Yet there are others who argue the contrary. They say that the loss of privacy is compensated for by the sheer convenience of the new technology and that the increased personal use of computers is, literally, returning us to the days of the village community, except that now it is a global village community.

51 The climate in which this debate takes place can also be critical. Particular events can be a catalyst, reducing as much as reinforcing the desire of individuals for privacy.

---

86 Hon Justice Michael Kirby "Privacy in Cyberspace" (1998) 21(2) U NSWLJ 323, 325 cited in Law Commission, above n 2, 71.

87 Office of the Privacy Commissioner "Privacy Protection: The Key to Electronic Commerce" (seminar delivered at the Asia-Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999, 1–4) cited in Law Commission, above n 2, 71.

88 David Feldman "Information and Privacy" in Jack Beatson and Yvonne Cripp (eds) *Freedom of Expression and Freedom of Information: Essays in Honour of Sir David Williams* (Oxford University Press, Oxford, 2000) 299.

89 It has since been replaced by the Data Protection Act 1998 (UK), which, in compliance with a European Union directive, extends to manual records.

90 Most directly in Principle 12 which relates to matching data by means of unique identifiers. This topic is usefully and lucidly discussed in *Report of the Privacy Commissioner for the Year Ended 30 June 2000* (Office of the Privacy Commissioner, Auckland, 2000) 65.

91 Above n 86 is one of the most vivid examples. However, the problem of hackers is best left to, and in New Zealand is dealt with by, the criminal law, as are the invasions of privacy committed by burglars and rapists.

52 Prior to the 11 September 2001 attacks on the World Trade Centre in New York and the Pentagon in Washington DC, many may have questioned how much personal information should be disclosed to law enforcement and national security agencies. Would they still be as concerned?

53 The evidence and findings of the Gisborne Cervical Screening Commission may be equally influential locally.[92] A woman who had had cervical smears carried out five years ago in Gisborne may have wanted the result to remain confidential. Now she may be prepared to have it recorded on a national database.

54 The following examples are some of the practical situations in which striking the appropriate balance between an individual's right to privacy and benefits for the whole community, or a significant section of it, is not straightforward:

- Is it appropriate for creditors in a liquidation to receive a list of other creditors with whom they can confer to appoint a liquidator? Or, are there weightier privacy interests, such as the fear that the information will be used to generate adverse credit reports?[93]
- Does the convenience of retail shopping online outweigh the disadvantage, which may be caused to an individual, of someone discovering that person has bought a product from a particular retailer?
- Is the greater security achieved through camera surveillance on various city streets worth the intrusion into the privacy of innocent passers-by?

55 Once the balance between competing interests is determined, the further question arises: how do we put these choices into effect without being oppressive? In some countries, local rules are being applied requiring Internet service providers and websites to filter their content.[94] But how effective are they? Firewalls are used in some countries to curtail the information that can be disseminated through the Internet. These may be more effective, but do they involve oppressive censorship?[95]

---

92 AP Duffy, DK Barrett and MA Duggan *Report of the Ministerial Inquiry into the Under-Reporting of Cervical Smear Abnormalities in the Gisborne Region* (Ministry of Health, Wellington, 2001).

93 As a matter of statutory interpretation, this point was resolved in favour of no disclosure of a list of creditors by Laurenson J in *Re Tasman Pacific Airlines of NZ Limited (In Receivership and In Liquidation)* (10 August 2001) High Court Auckland, M 1078/IM01.

94 "The Internet's New Borders" (11 August 2001) *The Economist* New York, 9–10. "Special Report: Geography and the Net: Putting it in its Place" (11 August 2001) *The Economist* New York, 11–20. A French judge recently ordered the Internet portal Yahoo! to find a way to stop French users from purchasing Nazi memorabilia on any of its sites, even sites in America.

95 "The Internet's New Borders", above n 94, see page 9 with particular reference to China, Singapore, Saudi Arabia, South Korea and Iran. But we doubt that a society such as New Zealand could tolerate the use of firewalls to deny access to such information.

WHAT IS PERSONAL INFORMATION?

56 The term "personal information", like "privacy", is not a legal term of art but, unlike "privacy", is susceptible to at least a working definition. It can be taken to mean information about a person, the disclosure of which he or she may reasonably expect to control.[96] The issue remains what constitutes a reasonable expectation?

57 The expectation may be inherent in the nature of the information. Most people regard information about their health, sexual behaviour or financial position as attracting such an expectation. Or the expectation may result from the circumstances in which the individual has disclosed the information, such as a letter marked confidential or the confession of a penitent to a priest, on the understanding that its dissemination will be restricted. Or, of course, both preconditions may exist, as is the case when a patient communicates information relevant to their mental health to a psychiatrist.

58 The expectation test is one that leaves little room for conclusive generalisation. For example:

- Sexual conduct that at one time and in some circles is regarded as not to be spoken of and shameful, at another time and in other circles may be freely discussed.
- There is now more candour about mental illness than there once was.[97]
- An individual may have no wish to conceal the fact that he or she has a broken rib, but may not wish to disclose that he or she is HIV positive.
- A politician may elect to tell the world about his or her state of health.
- Most of us are happy enough that our addresses should appear in electoral rolls and telephone directories. However, a witness or juror in a criminal trial fearful of gang retaliation, a battered wife who has fled from her husband, or a celebrity anxious to escape the attentions of fanatical admirers may reasonably expect to restrict her or his residential address.

59 Even where there is a relationship that would normally give rise to a reasonable expectation of confidentiality, there may be circumstances in which it is not justified. For example, there can be no reasonable expectation that a person in a relationship that imposes a duty of confidence will say nothing about acts performed *in public* by the party to whom he or she owes the duty.[98]

---

[96] This definition is we think neater than, but not different in substance from Professor Wacks' definition:

> "Personal information" consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation.

Raymond Wacks *Personal Information: Privacy and the Law* corrected paperback ed of 1st ed (Clarendon Press, Oxford, 1993) 26.

[97] But even so "a reasonable person of ordinary sensibilities would in the circumstances [plaintiff a public figure] also find publication of information that they had been a patient in a psychiatric hospital highly offensive and objectionable": *P v D* [2000] 2 NZLR 591, 601.

[98] *Woodward v Hutchins* [1977] 1 WLR 760, 762 in which the singer Tom Jones was refused an order restraining his former press agent from writing a newspaper article concerning "a very unsavoury incident in a Jumbo Jet" in which "Mr Tom Jones is said to have become inebriated and to have behaved outrageously on the aircraft".

60 Usually, the underlying purpose of the law regulating disclosure of information about an individual is to protect the particular individual's sensitivities. But is it possible to regulate the disclosure of information about an individual in a generic way? The diverse personality traits of human beings and the impossibility of generalising about when an expectation to control disclosure of personal information may be justifiable makes this difficult. The alternative is a case-by-case analysis that focuses on the specific factors of relevance in the particular circumstances.

WORKABILITY OF PERSONAL INFORMATION DISCLOSURE RULES

61 The New Zealand statute is along the same broad lines as legislation adopted in comparable jurisdictions. The Privacy Commissioner suggested in his 1998 report that "the Privacy Act is soundly based, and works well in operation", subject to the fine-tuning that he advocated in his review.[99] He said:

> My overall view of the Act is that it is well conceived and approaches the task in an appropriate manner. Naturally, there is room for improvement. Indeed, I have made over 150 recommendations. However, a study of our legislative history, and that of other similar jurisdictions, suggests to me that the Act is indeed firmly on the right track.[100]

62 An article published last year in the *New Zealand Herald*, as part of a series examining the whole issue of privacy, suggests that there remains a serious question about how well the Act works.[101] It concerned a 27-year-old account executive with an Auckland firm, who volunteered to be the subject of an experiment to show what personal information an ordinary person could find out given no more than the subject's name. The extent of what was discovered is astonishing.

63 If it is correct that despite the Privacy Act the sort of information described in this article is readily available, then what has the Act achieved? The answer may be that without the Act the subject's personal information would have been more easily discoverable or that even more secrets would have been revealed. Or perhaps people are misunderstanding and misapplying the Act and the law itself is not to blame.[102] How well does the Act work in practice? Is a better understanding of the Act and its application in practice required? If so, how is this achievable?

GROUNDS TO WITHHOLD PROTECTION

64 To what extent is it possible to define the circumstances in which legal protection for personal information should be excluded? We suggest that any disclosure of personal information must satisfy a threshold test of importance, for both the extent of the publication and importance to the complainant of the information,

---

99 Office of the Privacy Commissioner, above n 4, 11.

100 Office of the Privacy Commissioner, above n 4, 25.

101 Naomi Larkin and staff reporters "All about Lisa: A Life Laid Bare" (21–22 April 2001) *New Zealand Herald* Auckland, A3. The series on privacy ran from 21 April 2001 to 21 July 2001. A copy of the article is annexed as Appendix B. We are grateful to the *Herald* for permitting us to include this material.

102 Steven Price "Lessons in How Not to Be Caught in the Act" (15 January 2002) *The Evening Post* Wellington, 6.

to attract the attention of the law. Otherwise the protection offered by any statute runs the risk of being trivialised. An individual should not be entitled to invoke the protection of the law for every discourtesy or mildly wounding disclosure.

65 There are also public interest considerations. The very existence of the currently popular metaphor "whistle-blower"[103] demonstrates the widespread belief that there is a multitude of circumstances in which the public interest should prevail and disclosure should be allowed, despite the individual's expectation of being able to control the dissemination of personal information. The same belief underlies the provisions of the Protected Disclosures Act 2000, beyond the area of personal information.[104]

66 Further relevant examples include:

- The failure to disclose to close associates, such as flatmates, the information that a seemingly healthy person suffers from a psychotic illness that may lead to his or her committing violent assaults, perhaps if medication is not taken, has led to tragedy in recent New Zealand instances.
- What is the position of a medical practitioner whose patient persists in following his or her occupation as school bus driver, despite having been warned that he or she is likely to suffer, without warning, some devastating coronary or cerebral incident?
- Should someone who is HIV positive and who persists in engaging in unprotected sexual activities without disclosing that fact to his or her partner be entitled to insist that his or her state of health be kept confidential?
- Insurance fraud is difficult to detect. One way in which it can be detected is by insurance companies comparing notes and discovering patterns. Is it in the public interest that they should be able to do this, although normally what passes between insurer and insured is personal information and entitled to protection?
- Are there circumstances in which the public may have a legitimate reason to know even intimate information, such as, a Member of Parliament's choice of underpants?[105]
- What of the morals campaigner who engages in sexual activities inconsistent with his or her preaching?

67 The public interest issue may be expressed more broadly. The information that the individual seeks to suppress may not be merely personal, but also capable of discrediting them. An individual may seek to suppress it to avoid the disesteem of persons whose opinion matters to her or him. The information suppressed may affect the decisions of prospective employers, partners, customers or clients, friends, or even a prospective spouse. No doubt there is a public interest in allowing a repentant individual a fresh start, but some relationships call for warts-and-all disclosure.

---

[103] This term is used to describe an individual who breaches obligations of secrecy in the public interest.

[104] Protected Disclosures Act 2000, s 5.

[105] For readers outside of New Zealand, this is a reference to the media exposé of a former television network director's spending on clothing, including the purchase of a pair of underpants for $90. There was a legitimate public interest in this matter, because the television network was publically funded and the director was subsequently elected to Parliament, where he was sitting when the financial difficulties of the network that he had been a director of came to light. "Maori TV to be Audited after Spending Claims" (5 February 1997) *The Dominion* Wellington, 1.

68 Non-disclosure by a seller may shade into fraud:

> . . . people "sell" themselves as well as their goods. They profess high standards of behaviour in order to induce others to engage in social or business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character. There are practical reasons for not imposing a general legal duty of full and frank disclosure of one's material personal shortcomings – a duty not to be a hypocrite. But everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.[106]

Should the law facilitate such deception?

MODES OF PROTECTION

69 As with any rules interfering on one ground or another with the publication of statements of fact, the available legal mechanisms are one or both of:

- prior restraint; and
- sanctions after the event.

70 It is generally accepted that of the two options prior restraint is the more severe,[107] because it seriously impedes the free flow of information[108] and makes it impossible to test whether the restraint was warranted. In Professor Emerson's view:

> . . . a balance of considerations impels the conclusion that prior restraint should not be permitted in privacy tort cases. The controlling factor lies in the dynamics of that remedy. A prior restraint is so easy to apply and so destructive in its impact upon freedom of the press that its use cannot be justified. The only safe course is to confine restrictions upon the right to publish to an award of damages.[109]

71 Where should the choice between prior restraint and financial compensation after the event lie?

---

[106] Richard A Posner "The Right of Privacy" (1978) 12 Georgia L Rev393, 399–400.

[107] See, for example, the observations of the Court of Appeal in the context of objectionable material in *Living Word Distributors Limited v Human Rights Action Group Inc* [2000] 3 NZLR 570, 585; and see *R v Advertising Standards Authority Ltd* [1992] 1 WLR 1289, 1293; [1993] 2 All ER 202, 205 and *Douglas v Hello! Ltd* [2001] 2 WLR 992, 1032; [2001] 2 All ER 289, 327.

[108] This is why in defamation it is well settled that an injunction forbidding future publication of a statement claimed to be false and defamatory will not be granted where the publisher asserts that he or she can establish the truth of the statement.

[109] Thomas I Emerson "The Right of Privacy and Freedom of the Press" (1979) 14 Harv Civ Rights-Civ Lib L Rev 329, 349.

STATE INTERVENTION

72 Generally the law requires an individual seeking civil redress, such as damages or an injunction, to bring proceedings. There are exceptions to this general rule, which are frequently enacted for the benefit of the disadvantaged, but these are rare.[110]

73 If a personal statement is published that is untrue, a remedy exists in the law of defamation, but it must be pursued individually. If a personal statement is published that is true, but which reveals facts that an individual would have preferred not to be made known, should the Privacy Commissioner be available to help?

74 The Ontario Royal Commission took the view that a statutory tort was unlikely to provide an effective remedy for privacy problems because:

> The significant cost and uncertainty of success in bringing such claims would likely discourage aggrieved individuals from using a remedial device of this kind.[111]

No doubt it would. But is there a sufficient public interest to require the taxpayer to fund the pursuit of redress for those offended by such publications?

75 The law once enabled the Crown to seek sanctions, including imprisonment, against those who published criminal libels, defined as statements designed to insult any person or likely to injure his or her reputation by exposing him or her to hatred, contempt, or ridicule, or likely to injure him or her in his or her profession or trade. Truth was only a defence if the defendant could establish that the publication was for the public benefit. Otherwise even truthful disclosure of personal information was a criminal offence.[112] Criminal libel was abolished by the Defamation Act 1992 because it had "fallen into desuetude" in the view of the Committee on Defamation.[113] Yet the Privacy Act 1993 reinstated a form of penalty for the truthful disclosure of personal information.

76 Is it necessary or desirable for a government agency to take representative proceedings, on behalf of an individual with a grievance about the protection of personal information? Or is it preferable that the individual be left to pursue his or her own legal rights, as happens in the overwhelming majority of civil claims?

---

[110] The Commerce Commission is empowered to bring civil proceedings under the Fair Trading Act 1986 seeking redress for particular consumers. There are comparable provisions under the Human Rights Act 1993 and under the Privacy Act 1993. The Minister of Consumer Affairs recently announced that legislation is to be introduced empowering the Commerce Commission to seek redress from lenders for breaches of the law governing credit contracts: Hon Jim Anderton, Minister of Consumer Affairs "Consumer Credit Laws to Be Overhauled" (8 August 2001) Press Release.

[111] Ontario Royal Commission on Freedom of Information and Individual Privacy *Public Government for Private People* vol 3 *Protection of Privacy* (1980) 672 quoted in McBride, above n 15, 145, para 7.34. Mr McBride cites this position with approval.

[112] Crimes Act 1961, part 9. For criticisms of the law of criminal libel see JR Spencer "Criminal Libel – A Skeleton in the Cupboard" [1977] Crim LR 383 and 465; and "Criminal Libel in Action – The Snuffing of Mr Wicks" [1979] CLJ 60. Criminal libel was employed by Sir James Goldsmith in his campaign against *Private Eye*; see *Goldsmith v Pressdram Ltd* [1977] 1 QB 83; and for a description of Goldsmith's entire campaign and what provoked it see *Goldsmith v Speerings Ltd* [1977] 1 WLR 478.

[113] Committee on Defamation (IL McKay, Chairman) *Recommendations on the Law of Defamation: Report of the Committee on Defamation* (Government Printer, Wellington, 1977) 100.

OTHER OPTIONS

77 Finally, if in addressing the matters raised above, we conclude that improving our existing privacy law involves repealing the present statute, then we will need to consider whether there should be a statutory replacement. There are three possibilities:

- for the legislature to do nothing, leaving it to the courts to evolve a civil tort remedy for privacy breaches. As noted below, this is a pathway along which New Zealand courts have already set out;
- the creation of a blanket statutory tort under which the threatened publication of protected personal information, appropriately defined, could be forbidden by injunction, and actual publication could be penalised by an award of damages, if the court thought fit; or
- the creation of a series of more precisely targeted civil remedies.

78 These three options are not mutually exclusive. There is no reason why the development of a judge-made tort and the creation of statutory protections by the legislature for particular types of personal information or for particular methods of publication could not develop side-by-side.

79 In most United States jurisdictions, there exists a judge-made tort of privacy, or more accurately, four separate torts corresponding to the categories of privacy that we list in paragraph 2 of this paper. However, in Australia, the Law Reform Commission rejected a general privacy tort in favour of piecemeal attention to specific problems.[114]

80 In British courts, such developments also have been much more tentative than those in the United States. Fleming, in the last edition of his monumental work on torts, summed up the reasons for this caution in this way:

> Violation of privacy has not so far, at least under that name, received explicit recognition as a tort by British courts. For one thing, the traditional approach has been to formulate tort liability in terms of reprehensible conduct rather than of specified interests entitled to protection. For another, our courts have been content to grope forward cautiously along the grooves of established legal concepts, like nuisance and libel, rather than make a bold commitment to an entirely new head of liability. Some of this hesitation is undoubtedly due to the fact that we are here concerned primarily with injury in the shape of mental distress, which has so frequently evoked the fear of opening the door to fanciful claims. Another factor is the difficulty of drawing a clear line between what should and should not be tolerated. The mere fact of living in the crowded society of today exposes everyone to annoying contacts with others, most of which must be borne as the price of social existence. Also, free speech and dissemination of news are important competing values, and it is only when intrusion becomes intolerably offensive by prevailing standards of taste and proprietary that legal intervention would become warranted.[115]

---

[114] Australian Law Reform Commission *Privacy – No 22* (Australian Government Publishing Service, Canberra, 1983) para 1081. See also the recent High Court of Australia case, *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, para 186, where Kirby J confirms the majority decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 that no cause of action for breach of privacy exists in Australian common law.

[115] JG Fleming *The Law of Torts* (9 ed, Law Book Company Information Services, North Ryde, Australia, 1998) 664–665.

81 The New Zealand High Court is the exception in the Commonwealth to this guarded approach. In a series of judgments, of which the most influential was perhaps that of McGechan J in *Tucker v News Media Ownership Ltd*,[116] the Court has moved from statements agreeing that there is a need for a tort of public disclosure of private facts to an unqualified acceptance in the most recent reported case, *P v D*,[117] that such a tort now exists in New Zealand.[118]

82 A statutory tort of breach of privacy could be created and would address most of, what some argue are, the problems of the existing statute:

- There would be an end to the cost to agencies and to the taxpayer of the current regime, assuming that the enforcement of this new remedy would be by the aggrieved party.
- The law would develop on a case-by-case basis, which would end what some believe is the trivialisation of the issues that the current approach engenders. The courts would probably develop a threshold test of importance, for both the extent of the publication and the importance of the information to the complainant, which would prevent an individual from invoking legal protection for every trivial disclosure.
- An anticipated cautious judicial approach to the granting of injunctions ahead of publication may be a welcome alternative to the prior restraint that is the basis of the current scheme.
- If the statutory tort approach works for personal information, the experience acquired in the process will be valuable in assessing the possibility of extending the remedy to other classes of privacy.

83 But there are also strong contrary arguments:[119]

- There are formidable problems of definition and of identifying the circumstances in which the remedy should be withheld. An objective definition of the circumstances in which the remedy should be available is probably impossible:

  > The law should achieve the optimal amount of each of the conflicting values: protection of a person's intimate sphere without unduly limiting free expression. . . . This supposedly rational balancing of private and public interests remains a rather arbitrary procedure, in view of the inherent indeterminacy of the intended optimal solution; the latter is a wholly subjective value judgment on the "proper" societal concern.[120]

- A statutory provision would inhibit the free flow of information in general and impair media freedom in particular; the more imprecise the statutory definition, the more restrictive is its effect on freedom of expression.

84 The conclusion of the Australian Law Reform Commission concerning a general tort of privacy is equally applicable to a more limited tort confined to personal information:

---

116 [1986] 2 NZLR 716.

117 [2000] 2 NZLR 591.

118 There is a full account in S Todd *The Law of Torts in New Zealand* (3 ed, Brookers, Wellington, 2001) 920–925, para 17.5.4.

119 The solution of a blanket statutory tort was considered by T McBride in above n 15, 144–145, paras 7.32–7.35 and rejected by the then Minister of Justice, Geoffrey Palmer, in his foreword to the same work.

120 Izhak Englard *The Philosophy of Tort Law* (Dartmouth Publishing Company, Aldershot, 1993) 141.

> The Commission is not persuaded that it is appropriate to create a general tort of "invasion of privacy". Such a tort would be too vague and nebulous. It would need to be worked out, case by case, as courts and administrative tribunals grappled with particular fact situations that come before them. In time, perhaps, a set of principles might be developed through this process. The limits of the tort would ultimately be fixed. How it would affect freedom of the press, of speech and of information would only then be clear.[121]

85 The third option referred to in paragraph 77 is to attack specific problems. In a few United States jurisdictions, statute law seems to have developed in this way in parallel to the evolution of judge-made breach of privacy torts. As early as 1903, a New York statute made it both a misdemeanour and a tort to make use of an individual's name, portrait or picture for advertising or other trade purposes without consent.[122]

86 In New Zealand we are familiar with targeted privacy protections in the *criminal* law. Examples include:

- the offence of peeping and peering into a dwelling house at night without lawful excuse;[123]
- the offence of unlawfully opening a postal article;[124]
- the offence of monitoring private conversations by means of listening devices;[125]
- the provisions aimed at computer hacking presently being considered by Parliament;[126] and
- the statutory obligation on broadcasters to maintain standards consistent with "the privacy of the individual".[127]

87 A piecemeal approach has been proposed by the Australian Law Reform Commission:[128]

> If the courts would in time distil a general right down to specific principles why not do so immediately? If it is possible to define an area in which there is an undoubted claim for privacy protection, and where there is no legitimate claim for publication, legislation would be useful.[129]

---

121 Australian Law Reform Commission, above n 114, 24, para 1081.

122 1903 NY Laws Chap 132 § 1–2; triggered by the decision of the Court of Appeals in *Roberson v Rochester Folding-Box Co* (1902) 171 NY 538, 64 NE 442.

123 Summary Offences Act 1981, s 30(1)(a).

124 Postal Services Act 1998, s 23.

125 Crimes Act 1961, ss 216A–216E.

126 Crimes Amendment Bill (No 6) 1999, no 322-2, cls 250–251.

127 Broadcasting Act 1989, s 4(1)(c); discussed in *TV3 Network Services Ltd v Broadcasting Standards Authority* [1995] 2 NZLR 720.

128 Australian Law Reform Commission *Unfair Publication: Defamation and Privacy – No 11* (Australian Government Publishing Service, Canberra, 1999) ch 10, 123–135.

129 Australian Law Reform Commission, above n 128, 122.

There is Australian State legislation concerned with credit reporting agencies, for example.[130] As already mentioned, the creation in New Zealand of precisely focused remedies by statute would not displace developments that may occur in a judge-made code.

88 When can an individual reasonably expect the law to protect personal information about them? What countervailing interests outweigh the individual's right to privacy and should be exempted from legal protection? What is the best legal mechanism for the protection of personal information? How far, if at all, should the State be involved in protecting individual privacy?

---

[130] Invasion of Privacy Act 1971 (Queensland); Fair Credit Reports Act 1974 (South Australia) (later incorporated into the Fair Trading Act 1987); Credit Reporting Act 1978 (Victoria).

4
The issues

89 THE LAW COMMISSION has no wish to limit discussion on this paper to specific questions. We appreciate that submitters may prefer to address the matter either generally or under the three issues raised in the Terms of Reference. However, for those submitters who do prefer a list of specific questions we suggest the following issues:

i. Should there be any legislation at all to protect personal information?

ii. If yes, should it be:

- a statute along the lines of the Privacy Act 1993?
- a statute creating a blanket tort protecting personal information?
- a statute or statutes creating a series of precisely targeted civil remedies?
- or some other mechanism?

iii. If there is to be legislation, how should "personal information" be defined?

iv. What, if any, should the exceptions to the legal protection of personal information be?

v. Should the statutory protection of personal information exclude the trivial and unimportant?

vi. Should publication in the public interest be excluded from statutory privacy protection? How?

vii. Are there situations when the loss of individual privacy is outweighed by the convenience and/or benefit of disseminating the information? If so, what are these situations?

viii. Should the mode of statutory protection adopted be founded on prior restraint or the award of damages after the event?

ix. Should the enforcement of an individual's legal right to the protection of personal information be the responsibility of a State agency? Or should an individual be left to pursue her or his own legal rights?

x. Should a public interest in the enforcement of legal rights concerning privacy law be required for taxpayer-funded enforcement?

xi. What should constitute a sufficient level of public interest for publicly funded enforcement? How would this be determined?

xii. Would it adversely affect New Zealand's international relations or international trade if either the OECD guidelines are departed from or a model is adopted that is not regarded as "adequate" in terms of Article 25 of the EU Directive? If so, how?

xiii. How effective is the Privacy Act 1993? Is it working in practice? If not, provide examples of problems with the Act and, if possible, suggestions of how these problems may be resolved.

xiv. Is a better understanding of the Act and its application in practice required? If so, how is this achievable?

90 We look forward to receiving submissions.

APPENDIX A
Information Privacy Principles, Privacy Act 1993, part 2, section 6

Principle 1

Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 2

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

- (a) That the information is publicly available information; or
- (b) That the individual concerned authorises collection of the information from someone else; or
- (c) That non-compliance would not prejudice the interests of the individual concerned; or
- (d) That non-compliance is necessary—
  - (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) For the enforcement of a law imposing a pecuniary penalty; or
  - (iii) For the protection of the public revenue; or
  - (iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
- (e) That compliance would prejudice the purposes of the collection; or
- (f) That compliance is not reasonably practicable in the circumstances of the particular case; or
- (g) That the information—
  - (i) Will not be used in a form in which the individual concerned is identified; or
  - (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) The fact that the information is being collected; and

(b) The purpose for which the information is being collected; and

(c) The intended recipients of the information; and

(d) The name and address of—

(i) The agency that is collecting the information; and

(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law,—

(i) The particular law by or under which the collection of the information is so authorised or required; and

(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

(a) That non-compliance is authorised by the individual concerned; or

(b) That non-compliance would not prejudice the interests of the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That compliance would prejudice the purposes of the collection; or

(e) That compliance is not reasonably practicable in the circumstances of the particular case; or

(f) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4

Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) By unlawful means; or

(b) By means that, in the circumstances of the case,—

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 7

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) To request correction of the information; and

(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8

Accuracy, etc., of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary—

  (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

  (ii) For the enforcement of a law imposing a pecuniary penalty; or

  (iii) For the protection of the public revenue; or

  (iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—

  (i) Public health or public safety; or

  (ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information—
  (i) Is used in a form in which the individual concerned is not identified; or
  (ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—
(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary—
  (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  (ii) For the enforcement of a law imposing a pecuniary penalty; or
  (iii) For the protection of the public revenue; or
  (iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—
  (i) Public health or public safety; or
  (ii) The life or health of the individual concerned or another individual; or
(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or
(h) That the information—
  (i) Is to be used in a form in which the individual concerned is not identified; or
  (ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12

Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of [section OD 7 of the Income Tax Act 1994].

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

APPENDIX B
New Zealand Herald Article

ALL ABOUT LISA: A LIFE LAID BARE

21.04.2001 by Naomi Larkin and Staff Reporters

UNEARTHING THE PRIVATE LIFE of Lisa Barber took little in the way of digging.

Only hours after she granted her permission, a catalogue of her most personal and mundane details began to emerge – outlined by a paper trail of public records, and coloured in by unguarded public servants and retailers.

Lisa volunteered to be the subject of a Weekend Herald privacy investigation showing what an ordinary person, not a private eye or the police, could find from just a name.

She gave full agreement to having her life picked over – her employment, educational, financial, medical and personal details unravelled and exposed – because it was in the public interest.

The Weekend Herald's self-imposed rules were that neither Lisa nor her friends and family could be contacted. She was not to be followed or spied on or her mail opened.

Some calls were made on Lisa's behalf. But, if this newspaper could make such calls, so could some unscrupulous person pretending to be her.

An e-mail address and cellphone number were established to be Lisa's contact.

At each stage, she was kept informed.

There were areas, such as bank and medical records, where privacy laws were strictly observed, making access difficult.

But in other areas, privacy was overwhelmed by the human urge to gossip – the desire of the person on the other end of the phone line to give just a little more information.

The extent of the data uncovered has astounded the blond, 27-year-old former Southlander, who now lives in Auckland.

It ranges from her academic and Accident Compensation Corporation records, the Family Planning clinic she attends, her family tree dating back to the 1800s, through to what videos she was late in returning and how her hair was cut two years ago.

It even included information she was unaware of, such as a $383.43 tax rebate she had no idea she was owed.

The Weekend Herald found her e-mail address and was able, with some tips from hackers, to open it.

Today, Lisa Barber is a successful, key account executive for Tegel Foods in Auckland, but is heading overseas soon.

She happens to flat with a Weekend Herald reporter who took no part in the investigation.

Lisa became a houseowner at the age of 25 with her former partner, Matthew John Gibbs, who now lives in Australia. She bought her Mt Roskill three-bedroom, Californian bungalow in January 1999. It is now on the market.

When asked about the house, the former real estate agent also gave a description of Lisa: a blond woman of average height.

Auckland City Council property files show that rates bills of $1128.79 a year are to be sent to Heinz Watties in Victoria, Australia – obviously where her former partner now works.

Over the phone, a Mercury Energy staff member said the power account for the property was under her ex-partner's name with Lisa's present address given for any correspondence to be forwarded to.

Before buying, Lisa flatted in the suburbs of Mt Eden, Epsom and Grey Lynn. The Weekend Herald obtained all five previous addresses from a Baynet consumer credit search.

She now flats in Central Auckland.

She moved into the house, part-owned by one of the flatmates, this year and pays $100 rent plus expenses.

Lisa is an outgoing, sporty type. She is a registered member of the Health and Sports gym in Morningside, which has about 2000 members. A gym staff member said that under the Privacy Act they were not permitted to give out information, including confirmation of membership. However, this information – and the address of her Central Auckland flat – were provided by the staff member over the phone.

Her ACC records show the downside of her fitness regime. An ACC customer service representative at the 0800 inquiry centre told the Weekend Herald that to get their records a person must go into a branch office and present some form of identification such as a passport or driver's licence.

But as the representative talked, the information unfolded – read from a computer screen.

The data revealed a record of claims dating back to a dental injury in 1988. Other claims include sprain/strain of hand and wrist (twice) and thumb in 1992 and an ankle injury a year later.

The 1992 claims coincided with a dismal first year at Otago University, when her record is littered with fail, aegrotat and absent grades, suggesting that the hand and wrist injuries may have made it hard to write.

Her education records show the Gore-born former Southland Girls High School pupil was otherwise an above-average student. She graduated with Bachelor of Arts and Commerce degrees and a Diploma for Graduates in Management from Otago, with mainly A and B grades. The records were obtained from the university, in part using the established e-mail address.

Both of Lisa's parents are still alive. She has a younger brother and a sister, who is married with a daughter.

The minutiae of her private life, which shocked her most, came mainly from simple phone calls to her neighbourhood stores.

Two of the three video stores contacted by the Weekend Herald faxed details of what she had hired, even though Lisa uses her former partner's card in one. Videon refused to provide the information without a password.

Lisa is a regular video user, enjoying mainstream films rather than action or drama.

She is consistently late in returning videos.

In September 1999, she paid $34 to have her hair cut, "an inch off all over around face, vertical layers," according to computer records at Rodney Wayne Hairdressing, St Lukes.

She bought two $30 tickets from Ticketek for the ventriloquist Strassman's show at the St James Theatre on February 15. She belongs to the Automobile Association.

The St Lukes Family Planning clinic holds her "full" records, however a signed consent form is needed for these to be released.

Her Visa records also revealed a medical specialist she has been seeing.

Other personal financial details were reassuringly difficult to find out, as banks required customer identification numbers or account numbers.

But with her authority to use her WestpacTrust Visa card number – along with previously discovered public records such as date of birth and mother's maiden name – the Weekend Herald got a verbal list of recent transactions over the telephone.

They show Lisa owes $6213.36 on her account, shops at Foodtown Mt Eden, drinks wine, regularly uses taxis, flew to see her family in Invercargill this month and is not averse to a coffee at Starbucks.

She is obviously planning a trip overseas, having spent $2706.65 at the Newmarket Flight Centre and $104 at the Youth Hostel Association last month. A further $121 spent at the British High Commission indicates her destination is either Britain and/or Europe and is likely to be a working holiday.

She has no outstanding court fines.

Lisa has a work e-mail address and a Hotmail address. It was easy enough to find it – Lisa uses a common trick for her e-mail address – and get in.

The Weekend Herald spoke to – but did not engage – a hacker, who said a large number of people tended to use the word "password" or their middle names as their password. Lisa used "Maree."

Inside were the e-mail addresses of 49 family and friends, plus their nicknames. After she was told her e-mail had been accessed, Lisa changed the password. This could not be discovered.

Access to Lisa's e-mail would give a potential pursuer a huge ability to gather more information.

Her job history was uncovered under the guise of the Weekend Herald looking at employing Lisa.

She was a consultant for Sheffield Consulting Group, Auckland, from January 1997 to April 1999.

A person phoned at Sheffield disclosed that during this time Lisa and her former partner had a relationship problem. He moved to Australia 18 months later.

From May 1999 to June 2000, she was a trade business analyst for Meadow Lea Foods in Pakuranga.

This was one of the few organisations which requested that Lisa confirm that the information requested could be released. This was done via the established e-mail.

The Weekend Herald's investigation reveals that a complex picture of a person can be assembled by the easiest means.

It did not require private investigators, or sophisticated tracking devices or hacking into Government databases to uncover the most intimate details about an ordinary person.

If this newspaper can obtain so much through scrupulously controlled questioning, how much more could be found by the unscrupulous?

This information is out there – about you.

LISA BARBER

- Lists 49 friends on her Hotmail. We know their nicknames. We know the addresses.
- IRD owes her a tax refund of $383.43. She never knew until we told her.
- On February 15, 2000, she saw the ventriloquist Strassman at the St James. Sat in row A7, seat 6 in the Grand Circle.
- In 1992, she sprained hand and wrist in a sports accident. It was her first year at Otago University. Had to sit special exams because she could hardly write.
- Graduated with a Bachelor of Commerce degree in 1995, a BA and a Diploma for Graduates in Management in 1997. Got 10 A grades.
- On November 4, she babysat a child. They watched videos, the Tweenies and Sesame Street tapes.
- Pays $100 rent. Has lived in five flats in Auckland.
- We know her gym, a medical specialist, a former hairdresser, all about her house, her former partner.

OTHER LAW COMMISSION PUBLICATIONS

Report series

NZLC R1	Imperial Legislation in Force in New Zealand (1987)
NZLC R2	Annual Reports for the years ended 31 March 1986 and 31 March 1987 (1987)
NZLC R3	The Accident Compensation Scheme (Interim Report on Aspects of Funding) (1987)
NZLC R4	Personal Injury: Prevention and Recovery (Report on the Accident Compensation Scheme) (1988)
NZLC R5	Annual Report 1988 (1988)
NZLC R6	Limitation Defences in Civil Proceedings (1988)
NZLC R7	The Structure of the Courts (1989)
NZLC R8	A Personal Property Securities Act for New Zealand (1989)
NZLC R9	Company Law: Reform and Restatement (1989)
NZLC R10	Annual Report 1989 (1989)
NZLC R11	Legislation and its Interpretation: Statutory Publications Bill (1989)
NZLC R12	First Report on Emergencies: Use of the Armed Forces (1990)
NZLC R13	Intellectual Property: The Context for Reform (1990)
NZLC R14	Criminal Procedure: Part One: Disclosure and Committal (1990)
NZLC R15	Annual Report 1990 (1990)
NZLC R16	Company Law Reform: Transition and Revision (1990)
NZLC R17(S)	A New Interpretation Act: To Avoid "Prolixity and Tautology" (1990) (and Summary Version)
NZLC R18	Aspects of Damages: Employment Contracts and the Rule in *Addis v Gramophone Co* (1991)
NZLC R19	Aspects of Damages: The Rules in *Bain v Fothergill* and *Joyner v Weeks* (1991)
NZLC R20	Arbitration (1991)
NZLC R21	Annual Report 1991 (1991)
NZLC R22	Final Report on Emergencies (1991)
NZLC R23	The United Nations Convention on Contracts for the International Sale of Goods: New Zealand's Proposed Acceptance (1992)
NZLC R24	Report for the period 1 April 1991 to 30 June 1992 (1992)
NZLC R25	Contract Statutes Review (1993)
NZLC R26	Report for the year ended 30 June 1993 (1993)
NZLC R27	The Format of Legislation (1993)
NZLC R28	Aspects of Damages: The Award of Interest on Money Claims (1994)
NZLC R29	A New Property Law Act (1994)
NZLC R30	Community Safety: Mental Health and Criminal Justice Issues (1994)
NZLC R31	Police Questioning (1994)
NZLC R32	Annual Report 1994 (1994)
NZLC R33	Annual Report 1995 (1995)
NZLC R34	A New Zealand Guide to International Law and its Sources (1996)
NZLC R35	Legislation Manual: Structure and Style (1996)
NZLC R36	Annual Report 1996 (1996)
NZLC R37	Crown Liability and Judicial Immunity: A response to *Baigent's* case and *Harvey v Derrick* (1997)
NZLC R38	Succession Law: Homicidal Heirs (1997)
NZLC R39	Succession Law: A Succession (Adjustment) Act (1997)

NZLC R40 Review of the Official Information Act 1982 (1997)

NZLC R41 Succession Law: A Succession (Wills) Act (1997)

NZLC R42 Evidence Law: Witness Anonymity (1997)

NZLC R43 Annual Report 1997 (1997)

NZLC R44 Habeas Corpus: Procedure (1997)

NZLC R45 The Treaty Making Process: Reform and the Role of Parliament (1997)

NZLC R46 Some Insurance Law Problems (1998)

NZLC R47 Apportionment of Civil Liability (1998)

NZLC R48 Annual Report (1998)

NZLC R49 Compensating the Wrongly Convicted (1998)

NZLC R50 Electronic Commerce Part One: A Guide for the Legal and Business Community (1998)

NZLC R51 Dishonestly Procuring Valuable Benefits (1998)

NZLC R52 Cross-Border Insolvency: Should New Zealand adopt the UNCITRAL Model Law on Cross-Border Insolvency? (1999)

NZLC R53 Justice: The Experiences of Māori Women: Te Tikanga o te Ture: Te Mātauranga o ngā Wāhine Māori e pa ana ki tēnei (1999)

NZLC R54 Computer Misuse (1999)

NZLC R55 Evidence (1999)

NZLC R56 Annual Report (1999)

NZLC R57 Retirement Villages (1999)

NZLC R58 Electronic Commerce Part Two: A Basic Legal Framework (1999)

NZLC R59 Shared Ownership of Land (1999)

NZLC R60 Costs in Criminal Cases (2000)

NZLC R61 Tidying the Limitation Act (2000)

NZLC R62 Coroners (2000)

NZLC R63 Annual Report 2000 (2000)

NZLC R64 Defaming Politicians: A Response to *Lange v Atkinson*

NZLC R65 Adoption and Its Alternatives: A Different Approach and a New Framework (2000)

NZLC R66 Criminal Prosecution (2000)

NZLC R67 Tax and Privilege: Legal Professional Privilege and the Commissioner of Inland Revenue's Powers to Obtain Information (2000)

NZLC R68 Electronic Commerce Part Three: Remaining Issues (2000)

NZLC R69 Juries in Criminal Trials (2001)

NZLC R70 Acquittal Following Perversion of the Course of Justice (2001)

NZLC R71 Misuse of Enduring Powers of Attorney (2001)

NZLC R72 Subsidising Litigation (2001)

NZLC R73 Some Criminal Defences with Particular Reference to Battered Defendants (2001)

NZLC R74 Minority Buyouts (2001)

NZLC R75 Annual Report 2001 (2001)

NZLC R76 Proof of Disputed Facts on Sentence (2001)

NZLC R77 The Future of the Joint Family Homes Act (2001)

Study Paper series

NZLC SP1 Women's Access to Legal Services (1999)

NZLC SP2 Priority Debts in the Distribution of Insolvent Estates: An Advisory Report to the Ministry of Commerce (1999)

NZLC SP3 Protecting Construction Contractors (1999)

NZLC SP4 Recognising Same-Sex Relationships (1999)

NZLC SP5 International Trade Conventions (2000)

NZLC SP6 To Bind their Kings in Chains: An Advisory Report to the Ministry of Justice (2000)

NZLC SP7 Simplification of Criminal Procedure Legislation: An Advisory Report to the Ministry of Justice (2001)

NZLC SP8 Determining Representation Rights under Te Ture Whenua Māori Act 1993: An Advisory Report for Te Puni Kōkiri (2001)

NZLC SP9 Maori Custom Values in New Zealand Law (2001)

NZLC SP10 Mandatory Orders Against the Crown and Tidying Judicial Review (2001)

NZLC SP11 Insolvency Law Reform: Promoting Trust and Confidence: An Advisory Report to the Ministry of Economic Development (2001)

Preliminary Paper series

NZLC PP1 Legislation and its Interpretation: The Acts Interpretation Act 1924 and Related Legislation (discussion paper and questionnaire) (1987)

NZLC PP2 The Accident Compensation Scheme (discussion paper) (1987)

NZLC PP3 The Limitation Act 1950 (discussion paper) (1987)

NZLC PP4 The Structure of the Courts (discussion paper) (1987)

NZLC PP5 Company Law (discussion paper) (1987)

NZLC PP6 Reform of Personal Property Security Law (report by Prof JH Farrar and MA O'Regan) (1988)

NZLC PP7 Arbitration (discussion paper) (1988)

NZLC PP8 Legislation and its Interpretation (discussion and seminar papers) (1988)

NZLC PP9 The Treaty of Waitangi and Māori Fisheries – Mataitai: Nga Tikanga Māori me te Tiriti o Waitangi (background paper) (1989)

NZLC PP10 Hearsay Evidence (options paper) (1989)

NZLC PP11 "Unfair" Contracts (discussion paper) (1990)

NZLC PP12 The Prosecution of Offences (issues paper) (1990)

NZLC PP13 Evidence Law: Principles for Reform (discussion paper) (1991)

NZLC PP14 Evidence Law: Codification (discussion paper) (1991)

NZLC PP15 Evidence Law: Hearsay (discussion paper) (1991)

NZLC PP16 The Property Law Act 1952 (discussion paper) (1991)

NZLC PP17 Aspects of Damages: Interest on Debt and Damages (discussion paper) (1991)

NZLC PP18 Evidence Law: Expert Evidence and Opinion Evidence (discussion paper) (1991)

NZLC PP19 Apportionment of Civil Liability (discussion paper) (1992)

NZLC PP20 Tenure and Estates in Land (discussion paper) (1992)

NZLC PP21 Criminal Evidence: Police Questioning (discussion paper) (1992)

NZLC PP22 Evidence Law: Documentary Evidence and Judicial Notice (discussion paper) (1994)

NZLC PP23 Evidence Law: Privilege (discussion paper) (1994)

NZLC PP24 Succession Law: Testamentary Claims (discussion paper) (1996)

NZLC PP25 The Privilege Against Self-Incrimination (discussion paper) (1996)

NZLC PP26 The Evidence of Children and Other Vulnerable Witnesses (discussion paper) (1996)

NZLC PP27 Evidence Law: Character and Credibility (discussion paper) (1997)

NZLC PP28 Criminal Prosecution (discussion paper) (1997)

NZLC PP29 Witness Anonymity (discussion paper) (1997)

NZLC PP30 Repeal of the Contracts Enforcement Act 1956 (discussion paper) (1998)

NZLC PP31 Compensation for Wrongful Conviction or Prosecution (discussion paper) (1998)

NZLC PP32 Juries in Criminal Trials: Part One (discussion paper) (1998)

NZLC PP33 Defaming Politicians: A response to *Lange v Atkinson* (discussion paper) (1998)

NZLC PP34 Retirement Villages (discussion paper) (1998)

NZLC PP35 Shared Ownership of Land (discussion paper) (1999)

NZLC PP36 Coroners: A Review (discussion paper) (1999)

NZLC PP37 Juries in Criminal Trials: Part Two (discussion paper) (1999)

NZLC PP38 Adoption: Options for Reform (discussion paper) (1999)

NZLC PP39 Limitation of Civil Actions (discussion paper) (2000)

NZLC PP40 Misuse of Enduring Powers of Attorney (discussion paper) (2000)

NZLC PP41 Battered Defendants: Victims of Domestic Violence Who Offend (discussion paper) (2000)

NZLC PP42 Acquittal Following Perversion of the Course of Justice: A Response to *R v Moore* (discussion paper) (2000)

NZLC PP43 Subsidising Litigation (discussion paper) (2000)

NZLC PP44 The Future of the Joint Family Homes Act (discussion paper) (2000)

NZLC PP45 Reforming the Rules of General Discovery (discussion paper) (2000)

NZLC PP46 Improving the Arbitration Act 1996 (discussion paper) (2001)

NZLC PP47 Family Court Dispute Resolution (discussion paper) (2002)

NZLC PP48 Some Problems in the Law of Trusts (discussion paper) (2002)