



Privacy Commissioner  
Te Mana Matapono Matatapu

DP 12

REVIEW OF THE PRIVACY ACT 1993  
DISCUSSION PAPER No. 12  
**NEW PRIVACY PROTECTIONS**

---

The Privacy Commissioner is reviewing the operation of the Privacy Act under section 26 of the Act. The Commissioner will consider whether any amendments to the Act are necessary or desirable and will report his findings to the Minister of Justice.

This paper is one in a series which will cover the entire scope of the Act and highlight some issues. To find out which other discussion papers have been released, and to obtain copies of them, you may contact the Commissioner's office. Copies of the discussion papers will also be available through the Commissioner's web site.

---

The Privacy Commissioner welcomes comments on this paper and seeks responses to any specific questions raised. Submissions should be made in writing and be forwarded to the Commissioner's office by post or email no later than **10 November 1997**.

The Commissioner will hold a series of consultation meetings in the main centres and some regional cities during November. If you would like to be invited to a consultation meeting please indicate this with your written submission.

---

**Contact details for consultation**

Privacy Act Review  
Office of the Privacy Commissioner  
P O Box 10-094  
Wellington

fax: 04-474 7595 privacy hotline: 0800-803 909 email: [privacy@actrix.gen.nz](mailto:privacy@actrix.gen.nz)

For general enquiries about the review please speak to the Enquiries Officers at the freephone number. If you have a more detailed enquiry concerning your submission or the review please speak to the Codes and Legislation Officer at 04-474 7597.

Background materials on the Privacy Act available on the Internet at:  
<http://www.knowledge-basket.co.nz/privacy/welcome.htm>

ISBN 0-478-10367-0 1 September 1997

## INTRODUCTION

The purpose of this discussion paper is to consider whether there should be any new provisions or protections in the Privacy Act that have no present equivalent. The scope and therefore the focus has largely been restricted to consideration of:

- what other privacy laws and sets of privacy principles do and say;
- the European Union Directive on data protection.

The second point is included because our privacy law will be scrutinised by EU countries to see if it has “adequate” protections similar to provisions in the Directive.

This paper tries to avoid discussing other privacy laws and principles which simply say things *differently* to the Privacy Act - the focus is upon matters on which our Act is largely silent.

The paper also tries to focus upon ideas which may have some merit - provisions generally seen as having little merit, such as costly registration processes, are not considered in detail notwithstanding they have no direct equivalent in our Act. However this should not be taken as any indication that the Commissioner favours any particular suggestion. He has taken no position on the issues put forward in this discussion paper.

By and large this discussion paper has not tried to develop original ideas for privacy protection. It instead draws upon ideas which exist in the laws of other countries or which are included in sets of principles developed internationally or in other jurisdictions. Ideas are welcomed for entirely new privacy protections regardless of whether they are raised here.

## NEW PRINCIPLES

The information privacy principles are based upon 1980 OECD guidelines<sup>1</sup> which represent a culmination of 1970s thinking on information privacy issues. The OECD guidelines continue to be well respected internationally and many believe that they have stood the test of time in excellent fashion. They attempted, reasonably successfully, the difficult challenge of being "technology neutral" and suiting a wide variety of circumstances and jurisdictions.

However, from the early 1990s the OECD principles have been subject to criticism from several quarters.<sup>2</sup> It has been suggested that they are not as technologically-neutral as first supposed with some key concepts, such as "data controller" (or in the Act an "agency which holds information") based upon existing information storage media, such as a mainframe computer, rather than distributed computer networks or the Internet.

Even ardent supporters of the OECD guidelines have seen room for the development of new principles. The OECD has, for example, developed further guidelines on both security of information systems and encryption, each containing new principles. Our own Privacy Act has further and more specific principles in the public register privacy principles and the information matching guidelines. There has been concern to ensure that principles are up to the challenge of the "global information infrastructure" or "information society" as represented by the Internet, multimedia, and the convergence of a variety of technologies.

The suggestions that follow draw upon sets of privacy principles that have been developed in recent years in other jurisdictions. They have not been invented for the purpose of this discussion paper but represent the accumulation of detailed study and thinking elsewhere.

### Principles or sections in the Act?

Some thought should be given to the qualities which make a principle suitable for inclusion. It may be that some issues are better addressed through sections in the Act rather than principles. For example, the Act presently deals with information matching as a discrete matter through Part X rather than by having a principle on data matching.

Any new principle could have the following qualities:

- relevance to most agencies rather than touching upon an issue peculiar to just a few;
- capable of being clearly expressed in a length not exceeding any of the existing principles;

<sup>1</sup> OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows. These guidelines, and the OECD Guidelines on Information Security Management and the EU Directive on Data Protection mentioned below, are each reprinted in Butterworths, *Privacy Law and Practice*, Wellington.

<sup>2</sup> See, for example, John Gaudin "The OECD Privacy Principles - can they survive technological change?" (1997) 3 *Privacy Law and Policy Reporter* 143.

- relevance to personal information handling so as to fit with the existing principles.

**Q1. If new principles are to be considered for inclusion what qualities should they possess?**

### **Openness as to information policy**

The Hong Kong Personal Data (Privacy) Ordinance 1995 includes the following principle:

***“Information to be generally available***

All practicable steps shall be taken to ensure that a person can:

- ascertain a data user’s policies and practices in relation to personal data;
- be informed of the kind of personal data held by a data user;
- be informed of the main purposes for which data held by a data user are or are to be used.”<sup>3</sup>

The principle goes further than our own principle 3 in that it is not linked to a collection of information directly from the individual. It obliges agencies to be generally open as to their policies and practices in relation to personal data. This could go beyond the items listed in principle 3(1) and might include, for instance, an agency’s policies in respect of retention and archiving of personal information.

The Australian Privacy Charter contains a similar, although less precise, principle:

***“Openness***

There should be a policy of openness about the existence and operation of technologies, administrative systems, services or activities with potential to interfere with privacy.”

The principle explains that openness is needed to facilitate public participation in assessing justification for technologies, systems or services; to identify purposes of collection; to facilitate access and correction by the individual concerned; and to assist in ensuring that principles are observed.

**Q2. Is a new principle, not linked to collection, desirable in respect of openness regarding agency information practices?**

### **Anonymity**

The entitlement of individuals to enter into transactions on a basis of anonymity has been widely discussed in privacy circles over the last five years. The issue has become particularly pressing as many everyday cash transactions become replaced with EFTPOS and, in the near future, “electronic cash” transactions (whether on the Internet or by use of smart cards). The electronic transactions which are replacing cash

<sup>3</sup> Personal Data (Privacy) Ordinance 1995, Schedule 1, principle 5.

transactions each leave a trail of personal information. Technology exists to retain that information, assemble it, and enable its use for profiling and surveillance of individuals.

These issues are not brand new and the existing principles can, to a degree, grapple with them. However, entering into a transaction on an anonymous basis may be more effective to preserve privacy than simply trusting agencies to follow the principles. The choice for individuals to pay cash anonymously appear to be diminishing and the point may be reached in the next decade whereby, for practical purposes, they will cease to exist in any meaningful way.

Proponents of rights to anonymity would have the designers of electronic transactions build in an option of anonymity. The use of the telephone can illustrate this. Traditionally public telephones operated on the basis of coins. For a directly placed call there was no personal information generated or collected about the caller. Calls may now be made through the use of phonecards, credit cards, and telephone company issued calling cards. The coin phone and the phonecard are the anonymous transaction choices. The calling card leaves a data trail through the telephone company whereas the credit card call also leaves a trail through the financial system. While there is presently a choice of anonymity, at some future point this option might be dropped.<sup>4</sup>

With calls to introduce such things as electronic road tolls it could be seen as important from a privacy perspective that an option of anonymity be provided if our society is to avoid potential for massive data surveillance.

The US National Information Infrastructure (NII) principles<sup>5</sup> include the following:

***“Empowerment principle***

Individuals should be able to safeguard their own privacy by having ... the opportunity to remain anonymous when appropriate.”

The Australian Privacy Charter states:

***“Anonymous transactions***

People should have the option of not identifying themselves when entering transactions.”

A committee of the House of Commons in Canada has recently recommended a Canadian Charter of Privacy Rights which would include the following specific right:

“Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.”<sup>6</sup>

<sup>4</sup> A similar set of issues arises with telephone subscriptions. In jurisdictions without free local calling the itemisation of calls on statements can cause vexed privacy issues.

<sup>5</sup> Privacy Working Group Information Policy Committee Information Infrastructure Task Force, “Privacy and the National Information Infrastructure: Principles for providing and using personal information”, 6 June 1995.

<sup>6</sup> Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where do we draw the line?*, Ottawa, April 1997, recommendation 2.

There would be the need in some circumstances to insist on identification so as to prevent a breach of the criminal law. The requirement for customer verification in the Financial Transactions Reporting Act 1996, designed to combat moneylaundering, illustrates this. The NII principle does have an inherent limit in the inclusion of the phrase "when appropriate". The Canadian provision acknowledges that anonymity can be denied where "reasonably justified".

**Q3. Would a principle to allow individuals the option of anonymity when entering transactions be desirable? What exceptions might be appropriate?**

#### **Reasons for decisions**

The Privacy of Information Bill contained one principle which was later dropped. This would have obliged public sector agencies, which had made a decision or recommendation in respect of an individual in his or her personal capacity, to give the individual a reasonable opportunity to request a written statement of findings on material issues of fact and the reasons for the decision or recommendation.<sup>7</sup> This principle was based upon s.23 of the Official Information Act 1982. It was left in the Official Information Act which solely covers the public sector (whereas the Privacy Act generally treats the public and private sectors equally).

There may be little point in revisiting this issue on the same basis as the principle in the original bill. There would be little benefit in simply transferring the provision from the Official Information Act since existing arrangements appear to be working satisfactorily. However, consideration could be given to applying a similar, but more limited, principle equally to the public and private sectors. The blurring of the line between the public and private sectors, contracting out or privatisation of public services, and a general desire to place both sectors on a level footing, might suggest that the exercise of this important personal right should not be available only against public sector agencies. On the other hand such a right might be seen as too closely linked to notions of "administrative law" or "public law" and therefore unsuitable to be applied in the private sector.

Any such principle applied to the private sector would probably be limited to certain kinds of decisions in respect of individuals. An example might be employment decisions given that the public and private sectors are now largely governed by the Employment Contracts Act on the same basis. However, perhaps any such rights should be located in the appropriate sectoral laws, such as the Employment Contracts Act, rather than an information law like the Privacy Act?

**Q4. Should there be a principle concerning reasons for decisions when an agency makes a decision or recommendation in respect of an individual in his or her personal capacity? Would that sit comfortably with the private sector?**

<sup>7</sup> This is a brief summary of an aspect of the principle. The full principle is found in Privacy of Information Bill, clause 8, principle 8.

## BROAD PRIVACY PRINCIPLES - BEYOND DATA PROTECTION

### Australian Privacy Charter

The Australian Privacy Charter is an important recent attempt to take a general set of privacy principles beyond the well trodden route of data protection principles as found in European and OECD instruments.<sup>8</sup> The Charter does not attempt to specify the appropriate means of implementing the principles and some may be at too general a level to be suitable for incorporation directly into law. However, many of the principles have no direct equivalent in our principles and are therefore raised for consideration here.

In addition to the openness and anonymous transaction principles mentioned earlier in this paper, the Charter includes the following principles:

***“Freedom from surveillance***

People have a right to conduct their affairs free from surveillance or fear of surveillance. ‘Surveillance’ means the systematic observation or recording of one or more people’s behaviour, communications, or personal information.

***“Privacy of communications***

People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places.

***“Private space***

People have a right to private space in which to conduct their personal affairs. This right applies not only to a person’s home, but also, to varying degrees, in the workplace, the use of recreational facilities and public places.

***“Physical privacy***

Interferences with a person’s privacy such as searches of a person, monitoring of a person’s characteristics or behaviour through bodily samples, physical or psychological measurement, are repugnant and require a very high degree of justification.

***“No disadvantage***

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions), nor be denied goods or services or offered to them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a nominal operating cost.”

**Q5. Are any new principles or provisions desirable based upon the Australian Privacy Charter?**

<sup>8</sup> The Charter was prepared by the Australian Privacy Charter Council, a non-governmental organisation, in 1994.

## Proposed Canadian Charter of Privacy Rights

The House of Commons Standing Committee on Human Rights and Status of Persons with Disabilities of the Canadian Parliament recommended in April 1997 that the Government of Canada enact a declaration of privacy rights to be called the Canadian Charter of Privacy Rights.<sup>9</sup> The Privacy Charter would take precedence over ordinary federal legislation and served as a benchmark against which the reasonableness of privacy infringing practices and the adequacy of legislation and other regulatory measures would be assessed. The Committee appeared keen to go beyond data protection to suggest a set of broad privacy principles. It was clearly impressed by the Australian Privacy Charter.

Emphasising broad privacy rights which extend beyond data protection, the proposed first clause setting out “fundamental privacy rights and guarantees” stated:

- “Everyone is entitled to expect and enjoy:
- physical, bodily and psychological integrity and privacy;
  - privacy of personal information;
  - freedom from surveillance;
  - privacy of personal communications;
  - privacy of personal space.”<sup>10</sup>

Inspired by the Canadian Charter, and mirroring our own New Zealand Bill of Rights Act, there was provision for “justification for exceptions” which states:

“Exceptions, permitting the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees is reasonable and can be demonstrably justified in a free and democratic society.”<sup>11</sup>

The Charter then expresses general obligations including:

- “The basic duties owed to others to ensure their privacy rights are adequately respected include:
- the duty to secure meaningful consent;
  - the duty to take all the steps necessary to adequately respect others’ privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
  - the duty to be accountable;
  - the duty to be transparent;
  - the duty to use and provide access to privacy enhancing technology;
  - the duty to build privacy protection features into technological designs.”<sup>12</sup>

The Charter then sets out two specific rights relating to personal information, being:

<sup>9</sup> The report is available on the Internet at: <http://www.parl.gc.ca/committees352/huso/reports/03-1997-04/toce.html>

<sup>10</sup> House of Commons Standing Committee, *op cit*, recommendation 2, clause 1.1. - 04/toce.html

<sup>11</sup> *Ibid*, recommendation 2, clause 2.

<sup>12</sup> *Ibid*, recommendation 2, clause 3.1.

"Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.

"Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified."<sup>13</sup>

Specific obligations related to information or privacy follow. Most of these are quite familiar and are reflected in our own information privacy principles. One provision which has no direct equivalent in our principles is:

"The duty not to disadvantage people because they elect to exercise their rights to privacy."<sup>14</sup>

**Q6. Are any new principles or provisions desirable based upon the proposed Canadian Charter of privacy rights?**

**Implementing broad privacy principles**

Both the Australian and the proposed Canadian Privacy Charters move beyond data protection issues, the "bread and butter" of existing privacy laws. As the Canadian committee put it:

"We do not believe that Canadians want ground rules to protect only their informational privacy, leaving the rest of their privacy rights to languish in a lawless frontier. Consequently, the protective framework we are proposing here will capture the full breadth of privacy, like a wide angled lens taking in a panoramic view, as opposed to the data protection framework ... which focuses, like a closeup lens, ... on informational privacy rights."<sup>15</sup>

It would be difficult to apply some of the principles contained in the Australian or Canadian charters directly as principles in our Act. Reasons include:

- difficulties of the subject matter;
- the existing principles in our Act, and the supporting legal infrastructure, are based upon data protection concepts;
- the high level statements of principle would require refinement, including the development of exceptions, before they would suit direct enforcement through the mechanisms of the Act.

Notwithstanding these and other difficulties it might be thought that a Privacy Act which cannot deal with such matters remains somewhat incomplete. Certainly the Australian principles have been well thought out and may well be worthy of implementation in some way.

One possibility would be to establish such principles in the Act and direct the Privacy Commissioner to have regard to them in carrying out his functions. The effect of

<sup>13</sup> *Ibid*, recommendation 2, clause 4.

<sup>14</sup> *Ibid*, recommendation 2, clause 5.1.

<sup>15</sup> *Ibid*, chapter 4.

doing this would be to give statutory direction as to some of the privacy values that should be taken into account when, for example, the Commissioner offers the Minister advice on proposed new legislation. The principles would not be applicable beyond the Privacy Commissioner although a well drafted set of principles might well be influential beyond their direct application.

If a set of broad privacy principles going beyond data protection were to be developed, and the Commissioner was required to have regard to them, the position would be similar to that spelt out in:

- section 13(1)(e), whereby the Commissioner is to have regard to certain Council of Europe recommendations when reviewing the public register principles; and
- section 14, which requires the Commissioner to have regard to certain matters.

**Q7. Is there value in developing within the statutory framework a set of broad privacy principles, going beyond the existing emphasis upon information privacy and data protection issues, as a guide to the Privacy Commissioner in the exercise of his functions?**

If a set of broad privacy principles suitable for New Zealand were to be developed it might be possible to apply them to agencies as well as the Commissioner. Given that the principles might be less suitable for direct enforcement than the existing information privacy principles, it might be appropriate to simply require agencies to "have regard to" such principles or to comply "as far as reasonably practicable". Already the privacy principles are applied in such a manner in respect of public registers.<sup>16</sup>

Depending upon what sort of set of principles were to be developed, it might be appropriate to apply some of the principles to all agencies and others solely to some class or other. For example, the Australian Charter "privacy of communications" principle might be suitable for all agencies. On the other hand, a principle touching upon anonymity might instead be applied to agencies which intend to undertake some new endeavour impacting on privacy (in other words, agencies would not be expected to create an anonymity option for any existing service but instead be required to have regard to the principle if proposing to develop or launch a significant new service).

A more limited proposal would be to require all public sector agencies to have regard to such principles. This would be linked to ideas of "good government" and the notion that governments must pay special regard to the rights of individuals. On this approach, the private sector would be free to disregard the principles so long as its activities could be kept with the information privacy principles.

**Q8. If a set of broad privacy principles, going beyond data protection issues, were to be developed, would it be appropriate to require agencies to have regard to them?**

<sup>16</sup> See Privacy Act, sections 7(6) and 60.

## EUROPEAN UNION DIRECTIVE ON DATA PROTECTION

Over the next few years New Zealand's privacy law, in common with laws and controls in other nations, will be subject to scrutiny from Europe as to their "adequacy". Although one can be relatively confident that the EU countries would consider the protection given by the Privacy Act to personal data to be "adequate" that is not to say that New Zealand's law has all the elements that a European law is required to have under the EU Directive on Data Protection.<sup>17</sup> Accordingly, the EU Directive may be a suitable setting to consider whether there is a case for new privacy protections.

One can identify several provisions of the EU Directive that have no equivalent control in our Act, including:

- *restrictions on onward transfers of personal information to third countries* - Article 26 of the Directive controls transfer of personal data received from the EU to countries having no privacy laws;
- *sensitive data* - Article 8 anticipates additional safeguards for "sensitive data";
- *automated individual decision* - Article 15 anticipates that individuals should have the right to know the logic involved in the taking of an automated decision concerning them;
- *notification* - Articles 18 to 21 deal with notification which is the EU term for registration.

### Transborder data flows

Transborder data flows were the prime reason for the involvement of the OECD in privacy issues. The approach of the OECD is illustrated by the preamble to its 1980 Guidelines which recognises that:

- although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
- automatic processing and transborder flows of personal data create new forms of relationships amongst countries and require the development of compatible rules and practices;
- transborder flows of personal data contribute to economic and social developments;
- domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.

The 1981 Council of Europe Convention also recognised in its preamble the necessity to reconcile "the fundamental values of the respect for privacy and free flow of information between people." In 1991 the Council amplified its approach by issuing Recommendations recognising that personal data should not be transferred into states which "are not in conformity" with the Convention unless necessary measures have been taken to respect principles in the Convention such as:

- contractual provisions reflecting Convention principles and with the data subject given the possibility to object, or;

<sup>17</sup> Directive 95/46/EC on the Protection of Individuals with respect to the Processing of Personal Data and on free movement of such Data, 24 October 1995.

- obtaining the data subject's free and informed consent in writing.

The Recommendations also suggest that measures should be taken to avoid data being subject to automatic transborder communication without the knowledge of the individuals concerned.<sup>18</sup>

A similar approach to that taken by the OECD and Council of Europe was taken in 1990 United Nations Guidelines for the Regulation of Computerised Personal Data Files. Accordingly, during the 1980s and early 1990s, the international approach to the issue of transborder data flows has been to encourage consistent privacy law in jurisdictions which may transmit, receive or process personal data, and so long as the relevant privacy laws are comparable, to thereby avoid the need to place any additional restrictions on transborder data flows. However, the international instruments all recognise that controls may be appropriate in exceptional cases primarily where a country does not "substantially observe" the guidelines or which would "circumvent: domestic privacy law (the OECD terminology) where there are no "reciprocal safeguards" (UN) or where there is not "equivalent protection" (Council of Europe). The international instruments give some guidance as to the types of control, or standard of control, where there is no substantial or equivalent protection in another jurisdiction. This usually involves contractual protections or individual consent.

The emphasis given in the respective OECD and European instruments has meant that most European privacy laws contain express transborder data controls whereas most laws based on the OECD Guidelines (like New Zealand) do not. Section 12 of the Data Protection Act 1984 (UK) provides an example of a law implementing the Council of Europe approach. That gives the UK Data Protection Registrar (equivalent to the Privacy Commissioner) a limited power to prevent personal data being transferred to a place outside the UK if satisfied that there is likely to be a contravention of one of the data protection principles as a consequence of the transfer.

Interest in the matter of transborder data flows was rekindled in the 1990s through the new involvement of the of European Union in privacy matters. The EU's approach has subtly changed the relatively relaxed way that the OECD and other bodies had tackled the issue and caused other jurisdictions to rethink their approach.

Article 25 of the EU's 1995 directive requires EU countries *must* provide that the transfer of personal data to third countries for processing may take place *only* if the third country ensures "an adequate level of protection". The importance of the EU in international trade has meant that this requirement has refocussed attention in a number of countries on whether their laws would be adequate in European eyes.

Transborder controls are being re-evaluated in EU countries which need to implement the directive in national law. Section 12 of the Data Protection Act 1984 (UK) may be inadequate to meet the Directive's requirements. The UK Data Protection Registrar in considering alternatives has stated:

---

<sup>18</sup> The 1981 Council of Europe Convention, and the 1991 Recommendations, are re-published in Butterworth's *Privacy Law and Practice*, Wellington, 1993-97, as is the EU Directive.

“Article 25.1 of the Directive imposes a duty on member states to ensure that transborder data flows to third countries take place only where there is adequate protection. In our view it is neither practical nor appropriate to regulate transborder data flows by some scheme of prior vetting. Instead we recommend that a duty be imposed on controllers [equivalent to “agencies” in the New Zealand Act], a prohibition against transferring data overseas unless article 25.1 is satisfied. Article 25.1 would therefore be transposed into UK law by transferring the duty imposed on member states to data users. The Registrar would commend as a model for this approach, section 33 of the Hong Kong Personal Data (Privacy) Ordinance [1995].”<sup>19</sup>

Jurisdictions outside Europe are looking to the possibility of transborder data flow controls not simply to protect the data of their own citizens but also to ensure that their jurisdictions are not perceived as conduits for transfers to “data havens” for which direct transfers would be banned.

The transborder data flow controls in section 33 of the Hong Kong law only take effect if the Hong Kong Ordinance ceases to apply.<sup>20</sup> Where the transfer of data is accompanied by a loss of control of the data, section 33 applies. This permits a transfer where it is to a jurisdiction possessing “any law which is substantially similar to, or serves the same purpose as, this Ordinance” and the Privacy Commissioner may specify such jurisdictions by Gazette notice. Also permitted are transfers justifiable on public interest grounds, or which further the interest of the individual concerned. However, in all other cases section 33 requires that the transferor should be subject to a duty to take all reasonable steps to ensure that the transferee applies similar data privacy standards to those applicable in Hong Kong. It will be for the transferor to assess the situation and take the most appropriate steps. Consideration has to be given to such measures as obtaining contractual assurances and in this respect the Hong Kong Commissioner has released a suitable model contractual conditions.<sup>21</sup> The Commissioner can receive complaints relating to alleged breach of the transferor’s duty. The Hong Kong prohibitions are also enforced by an enforcement notice procedure similar to provision in the UK.

**Q9. Should the Privacy Act include controls on the transfer of personal information to jurisdictions which do not apply a standard of protection comparable to those in the OECD guidelines? What factors should most influence the Privacy Commissioner in making any such recommendation? What issues should any recommended scheme particularly take account of?**

<sup>19</sup> Data Protection Registrar, *Our Answers*, response of the Data Protection Registrar to consultation paper on the EC Data Protection Directive (95/46/EC), July 1996, paragraph 13.5.

<sup>20</sup> To relate this to a New Zealand situation, section 10 of the Privacy Act 1993 makes it clear that the privacy principles continue to apply to certain information held by New Zealand agencies overseas. If the Hong Kong approach were to be taken, any special transborder data flow controls would only apply if the New Zealand agency relinquished control in terms of section 10. The discussion of the Hong Kong law is largely drawn from Berthold, “Hong Kong’s Personal Data (Privacy) Ordinance 1995”, *Privacy Law & Policy Reporter*, 2/9 December 1995, 166.

<sup>21</sup> Office of the Privacy Commissioner for Personal Data, Hong Kong, fact sheet no 1, “Transfer of Personal Data Outside Hong Kong: Some Common Questions”, May 1997.

**Q10. If a transborder data flow control is warranted, should it empower the Commissioner to take prohibition action in exceptional cases? Or should any provision place the responsibility on agencies which are contemplating transferring personal information out of the jurisdiction?**

The detail of a transborder data flow control has not been discussed here, except in passing in respect of the UK and Hong Kong models. It is not proposed to take the matter forward in any depth in this paper since it is thought better at this stage to concentrate on whether there should be any such control. However, if people preparing submissions have any thoughts on the mechanics of a transborder data flow control the Commissioner would be interested to hear them. The sort of matters which will have to be considered, if controls were to be recommended, would include:

- how jurisdictions with “adequate” privacy protections can be distinguished from those without - although Europe and Hong Kong propose preparing lists, it is anticipated that this will prove a difficult task;
- how any regime would be enforced.

In keeping with other aspects of the Privacy Act, it would be desirable that any scheme keeps compliance costs to a minimum. The comment of the UK Data Protection Registrar, who indicated that any scheme of prior vetting would be neither practical nor appropriate, is endorsed. A list of jurisdictions having adequate privacy law would probably enhance the ease of compliance and might therefore be a desirable feature. However, the administration costs, and other drawbacks, would probably suggest that a corresponding list of jurisdictions having inadequate privacy law should be avoided. Possibly New Zealand could take advantage of the EU work by deeming a jurisdiction recognised by the EU as having “adequate” privacy protection to have adequate privacy protection for any transfer from New Zealand.

**Q11. What test should any transborder data flow control apply? Should a distinction be made between OECD countries “substantially observing” the OECD guidelines and other countries which might be expected to have, say, “equivalent protection”? Is a listing system to distinguish jurisdictions desirable?**

### **Sensitive data**

Most European laws are based upon the Council of Europe Convention No 108 and include controls on sensitive categories of data. The EU Directive continues the previous approach and anticipates special controls for sensitive categories of data. The European approach is summarised by noting that “while the risk that data processing is harmful to persons generally depends not upon the contents of the data but on the context in which they are used, there are exceptional cases where the processing of

certain categories of data is as such likely to lead to encroachments on individual rights and interests.<sup>22</sup>

The OECD guidelines have much in common with the European approach but differ by not including reference to sensitive categories of data. Accordingly, laws derived from the OECD guidelines such as those in Canada, Australia and New Zealand have no such categorisation. There may also have been less consensus in the OECD as to what constituted "sensitive categories" compared with the Council of Europe. The European approach to sensitive categories is believed to have been heavily influenced by the European experiences of totalitarian regimes, particularly in the 1940s whereby data on individuals' race or religion had led to discrimination, torture and death.

In considering whether he ought to recommend special controls on sensitive categories of data, the Commissioner will need to consider several questions, including:

- will any such regime benefit privacy?
- what are the costs to be set against any such benefits?
- what would be "sensitive categories" of information in our society?
- what special controls would be applicable to sensitive categories?

The balance of this section will discuss those matters.

#### ***Costs and benefits of a "sensitive categories" regime***

Well designed controls relating to sensitive categories of data may well lead to enhanced standards of privacy for individuals. Sometimes if an individual is known to have some personal characteristic, such as membership of an unpopular minority group, that person may be subject to detriment or discrimination. Sometimes legal protection is extended to such people, as for example through the Human Rights Act. However, legal protections are not always effective and, in any case, redress comes after the event which may be of little comfort to the individual. Accordingly, an alternative strategy is sometimes to ensure that the individual is not marked out or identified as having the characteristic believed to lead to discrimination. The Human Rights Act, for example, prohibits employers from seeking certain information on which to base employment decisions.

Although the discussion here has been in terms of "sensitive categories" of information, it is an approach not dissimilar to that anticipated by information privacy principle 1 which requires that if an agency is to collect personal information it must be for a lawful purpose connected with a function or activity of the agency and the collection of the information must be necessary for the purpose. However, principle 1 does not put constraints on agencies' legitimate purposes (beyond what is "lawful") nor does it specify a strict standard for sensitive categories of information.

A second possible benefit of having special controls on sensitive categories of information is that it would remove one aspect where there is no equivalency between our law and the EU Directive. It may therefore strengthen our case that the New

<sup>22</sup> Council of Europe, explanatory report on the conventions for the *Protection of Individuals with Regard to Automatic Processing Data*, 1981, paragraph 43.

Zealand law is “adequate” in EU terms. While this is a positive feature, it is only of marginal importance as on any current reckoning the New Zealand law should pass any EU adequacy test with flying colours with, or without, special controls in relation to sensitive categories of data.<sup>23</sup>

Some negative aspects of having special controls relating to sensitive categories of information include:

- it may make the Act slightly more complicated - although, as discussed below, controls could be incorporated into existing mechanisms, such as codes of practice or regulations, thereby leading to no greater complications than exist at present;
- there may be some compliance or administration costs in the proposal - none have been identified and the effect is believed to be minor so long as, as suggested above, the proposal utilises existing mechanisms;
- it might over emphasise sensitive categories to the detriment of good information handling - the approach of the OECD and the information privacy principles has been to emphasise principled handling of *all* personal information not simply “sensitive categories”.<sup>24</sup>

**Q12. What are the positive reasons to impose controls on the handling of sensitive categories of personal information?**

**Q13. What are the negative features of special controls on sensitive categories of information? Do the positive features outweigh the negative of having such controls?**

### *Categorisation of sensitive data*

There is no worldwide consensus on what constitutes a full range of “sensitive categories”. If there were to be special controls in our Act it would be important to properly identify what is sensitive in New Zealand and not what the prevailing view in another society is.

The first international instrument to establish a list of sensitive categories was the Council of Europe Convention. Article 6 stated:

“Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.”

The Council of Europe has made it clear that the list is not meant to be exhaustive and states are permitted to include other categories of sensitive data. The list therefore is one in which *all* member states considered the data to be especially sensitive.

<sup>23</sup> It should be added that this is speculative. There has been no official EU review of New Zealand’s Privacy Act.

<sup>24</sup> In contrast of some traditional concepts such as confidentiality.

The Council explains:

“The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views.”<sup>25</sup>

The EU Directive contains a similar list. It states in article 8(1):

“Member states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.”<sup>26</sup>

If a list were to be drawn up in New Zealand several approaches could be taken. These might include:

- adopting a list which refers explicitly to the grounds for discrimination in the New Zealand Bill of Rights Act 1990;
- setting out in the Act itself a list along the lines of the European models but suitably modified for New Zealand conditions;
- introduces the concept of “sensitive information” without definition thereby permitting the matter to be further developed by the Privacy Commissioner explicitly through codes of practice;<sup>27</sup>
- providing in the Act for the Executive through regulations to declare the categories of sensitive information.

**Q14. If controls on sensitive categories of personal information were to be introduced, should the Act specify the categories of information or should a process be established for these to be determined later?**

**Q15. If the Act were to list sensitive categories of data, what categories should be listed?**

#### *Mechanisms dealing with sensitive categories*

The final issue would be the question of the controls to be applied to sensitive categories of data. It would be possible for the Act to be quite specific about what was prohibited (e.g. prohibiting the transfer of such data out of the jurisdiction except on certain conditions such as individual consent). If the Act were to specify this, there would also need to be some exceptions allowed which could also be set out in the Act. How extensive the exceptions would need to be may depend upon how broad the categories of data and the prohibitions or controls were.

<sup>25</sup> Council of Europe, *op cit*, paragraph 48.

<sup>26</sup> The balance of the article sets out a number of exceptions whereby processing of special categories of data is permitted.

<sup>27</sup> This, and the suggestion concerning regulations, will be further developed in the following section on mechanisms.

Alternatively, the Act could provide for controls which could be brought into force at an appropriate time. One approach would be to establish a mechanism whereby the government could, if it wished, issue regulations dealing with sensitive categories. For example, regulations could be issued prohibiting the transfer of a specified class of sensitive information subject to conditions set out in the regulations. This would give our law the framework whereby special controls could be introduced but would not itself make immediate change to implement those. Such regulations could be introduced at a later time following further study and consultation or they might be introduced in response to a particular development of public concern.

Another alternative would be to utilise the existing mechanisms of the Privacy Act to allow for sensitive categories of data to be addressed. The obvious way of doing this would be in respect of codes of practice. Indeed, already codes of practice can - and do - deal with sensitive categories of information although without assigning the information that label. For example, a major motivation in the issue of the Health Information Privacy Code was a concern over the sensitivity of medical and health care information.

Probably no special change to the law would be necessary to deal with sensitive categories of information in a general way through codes of practice. However, if very strong controls in respect of sensitive categories were deemed appropriate it might be preferable for this to be spelt out giving the Commissioner the appropriate power. Generally speaking, for the Commissioner to do something by code of practice it needs to be characterised as a "modification of the application of the information privacy principles" or to be prescribing how the principles are to be applied or complied with.<sup>28</sup> An attempt to totally prohibit the export of a particular class of data, or to prohibit its collection, use or disclosure, might well be subject to challenge as going beyond what might be contemplated by section 46. Accordingly, if special controls on sensitive categories of data are desired there may be a case to amend section 46 to set out additional matters that codes could do in relation to such sensitive categories.

**Q16. How best might a regime controlling sensitive categories of data best be implemented? Would the best approach involve a new part of the Act, the creation of regulation making powers, or an amendment to the powers to make codes of practice?**

### **Automated decision making**

The EU's automated individual decision requirements are apparently derived from French law and are not discussed here as the concepts seem rather alien to our present Act. It may be easier to evaluate the usefulness of such an approach in a couple of years when the obligation has been implemented at national level in common law countries such as Ireland and the UK.

---

<sup>28</sup> Section 46(2).

### **EU notification requirements**

The EU Directive contains provisions relating to what it terms "notification". It appears that notification is simply a new term for what has in the past been known as "registration". As earlier signalled in this paper, and in other discussion papers such as Discussion Paper No 9 on compliance costs, registration has been carefully examined and rejected in the New Zealand context as being undesirable in terms of effectiveness, administration and business compliance costs. It is not proposed to re-examine the issue here.

The Privacy Commissioner may include in his final report a list of submissions received. He may also refer to submissions in the text of his report. If you want your submission, or any part of it, treated confidentially, or do not want it used in this way, please indicate this clearly. The Commissioner is subject to the Official Information Act. Copies of submissions may therefore be released on request. Any request for the withholding of information on the grounds of confidentiality or for any other reason will be determined in accordance with that Act and section 116 of the Privacy Act.

*discuss/newprin*