

# Chapter 9

## Information matching

- 9.1 The State collects and holds a vast amount of personal information about its citizens. Some of the information is provided by citizens of their own accord. Most is acquired either by compulsion or in circumstances where a citizen has no choice but to provide the information if he or she wants to receive a service or benefit. And technology now provides the tools to use this huge store of information in ways never before possible. As one commentator has noted:<sup>609</sup>

it has become practical to manage, exchange, match and mine vast quantities of information about people and their personal lives, rapidly and without their involvement. The technological capacity and the bureaucratic imperative to record and report that it facilitates have far outpaced social change. It is like the Black Death: the population has no natural resistance and no real understanding of what is happening and why.

- 9.2 This chapter and the next relate to information matching and information sharing. Both are matters that relate exclusively or principally to the activities of public sector agencies rather than the private sector. While the two matters have a significant degree of overlap, each raises quite distinct issues.
- 9.3 Information sharing (or data sharing) is a wider term than information matching. Information sharing covers the situation where information is made available by one agency to another. Information sharing is covered by the ordinary privacy principles (except where another statutory provision applies). One of the key issues raised in the next chapter is whether the privacy principles are sufficiently clear or flexible to enable the sharing of information between government agencies when this is necessary or desirable in the public interest or the interests of an individual.
- 9.4 Information matching (or data matching) is in some respects a subset of information sharing, since it involves one agency making information available to another. In some cases the ordinary privacy principles would not prevent it. However, information matching has its own regime in the Privacy Act. It is dealt

---

609 Submission by No2ID, quoted in Richard Thomas and Mark Walport *Data Sharing Review Report* (2008) Annex C 26.

with in Part 10 and Schedules 3 and 4. Information matching essentially involves “the comparison of one set of records with another, generally with the aim of finding records in both sets that belong to the same person.”<sup>610</sup>

- 9.5 This chapter:
- looks at what information matching is, and why the Act contains a separate regime for it;
  - examines the existing provisions in the Act and whether or not they are working in practice;
  - looks at overseas approaches to information matching in Australia, Canada, the UK, the US, and Hong Kong, and whether there are any lessons to be learned; and
  - puts forward a number of suggestions for change.

---

## BACKGROUND What is information matching?

- 9.6 Part 10 and Schedules 3 and 4 of the Act relate to information matching by public sector agencies. Information matching essentially involves the (usually computerised) comparison of personal information from one source against personal information from another source, for the purpose of producing or verifying information about an identifiable individual. In most cases, the objective is to detect whether identifying information (usually a name) about the same individual appears in both sets of information. Occasionally, the fact that an individual’s information appears in only one set of information will be of interest. An objective often associated with information matching is the detection of fraud in the delivery and receipt of social assistance programmes such as social welfare benefits and student allowances. However, in some cases the objective may be to benefit the individual, such as identifying people who are eligible to vote but are not registered as electors, or people who are not claiming a social welfare benefit to which they are entitled. Over the years since information matching was first legislated for in New Zealand, there has been a shift towards purposes that are more beneficial to individuals than the original purpose of detecting and avoiding benefit fraud.
- 9.7 The primary purposes of information matching have been identified as being:<sup>611</sup>
- detection of errors in programme administration;
  - confirmation of continuing eligibility for a benefit programme, or compliance with a requirement for a programme;
  - detection of illegal behaviour by taxpayers, benefit recipients, government employees, and so on;
  - monitoring of grants and contract award processes;
  - location of persons with a debt to a Government agency;
  - identification of those eligible for a benefit but not currently claiming;
  - data quality audit; and
  - updating of data in one set of records based on data in another set.

---

610 Privacy Commissioner *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2009* (Office of the Privacy Commissioner, Wellington, 2009) 41.

611 Roger Clarke “Dataveillance by Governments: The Technique of Computer Matching” (1993), available at [www.rogerclarke.com](http://www.rogerclarke.com).

## Why is information matching dealt with specifically in the Act?

9.8 Authorising the exchange of information between certain government agencies for the purpose of combating fraud and abuse of the social welfare system, and subjecting those information exchanges to a system of controls, reporting, and monitoring, was one of the purposes of the Privacy of Information Bill introduced in 1991. Indeed, the desire of the then government to enact those authorisations without delay resulted in their being split off from the Bill and enacted separately, along with those parts of the Bill relating to the establishment, functions, and powers of the Privacy Commissioner. They were enacted as the Privacy Commissioner Act 1991, and later subsumed into the Privacy Act 1993.

9.9 The first Privacy Commissioner, Bruce Slane, commented that:<sup>612</sup>

the Privacy Act 1993 fulfils a function of legitimising information matching. In my view, it is an appropriate function of data protection legislation to legitimise data matching if it avoids the ad hoc and uncontrolled application of the technique and subjects the activity to a satisfactory set of controls embodying fair information practices.

He considered that Part 10 of the Act and the information matching rules “are the key safeguards to ensure authorised information matching programmes are carried out fairly and successfully and in a way that protects the interests of affected individuals.”<sup>613</sup>

9.10 There are both policy and technical issues relating to the use of information matching. The Privacy Commissioner has listed perceived negative impacts of information matching, including:<sup>614</sup>

- using information obtained for one purpose for an unrelated purpose;
- providing opportunities for “fishing” in government records with the hope of finding wrong-doing;
- initiating investigations without a pre-existing “cause to suspect”;
- presuming people guilty simply because they are listed in a computer file, requiring them to prove their innocence;
- multiplying the effects on individuals of errors in government databases;
- undermining trust by dispersing information obtained by one agency in confidence;
- disclosing an individual’s data without the individual’s knowledge;
- taking action against individuals based on incorrect information or incorrect matching;
- taking action against individuals without their knowledge; and
- removing common sense and human judgment if decisions are automated.<sup>615</sup>

---

612 Office of the Privacy Commissioner *Review of Statutory Authorities for Information Matching* (Wellington, 1999) para 3.2.1.

613 Office of the Privacy Commissioner *Amendment of Information Matching rules* (Wellington, 2001) para 2.2.

614 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 39; Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 41.

615 For an excellent discussion of the issues relating to automated decision-making and due process, see Danielle Citron “Technological Due Process” (2008) 85 Wash U L Rev 1249.

- 9.11 From a technical point of view, a simplistic view of information matching as merely comparing one set of data against another belies a number of serious issues. These are well summarised in the Privacy Commissioner's 2008 Annual Report:<sup>616</sup>

On the surface, using a computer to compare one set of records with another seems straightforward. However, this is rarely the case. For a start, the matching is usually against another organisation's information, which may mean a host of differences from a technical perspective as well as from organisational legal and even social perspectives. The two sets of data that are compared are likely to have been collected for different purposes, in different contexts and at different times, and may have different levels of detail, accuracy or format. For example, one data set may only contain the year of birth rather than the full date of birth, or may only contain informal preferred first names (aliases) rather than the full first names as listed on a passport. Seemingly objective characteristics such as address and declared income can differ on two databases for a variety of reasons, many of which do not indicate an intention to deceive anyone.

Through the process of comparing records from different sources, information matching seeks to discover new facts about an individual by inferring that two records relate to the same person. For example, finding that an individual on the list of beneficiaries appears to be the same individual shown on another department's list of travellers departing overseas, suggests that a beneficiary has travelled overseas. However, all that matching actually delivers is an inference that these records are likely to belong to the same person; the match alone cannot deliver certainty about this. Mismatches can arise from incomplete, inaccurate or simply similar data.

- 9.12 Information matching involves the transfer of vast amounts of personal information from one agency to another. This raises the risk of accidental or deliberate loss or disclosure of the data. Under the Privacy Act, online matching is not permitted unless the approval of the Privacy Commissioner is obtained, and conditions may be imposed on such approvals to safeguard the data involved. The 2009 Annual Report of the Privacy Commissioner reports that, as at 30 June 2009, online transfer was used in 26 of the 50 active data matching programmes.<sup>617</sup> With respect to programmes where data is physically transferred between agencies, the Privacy Commissioner has required that the data is encrypted to safeguard the security of the data if it is lost or stolen. The Privacy Commissioner reports that, as at 30 June 2009, 19 matching programmes involve physical transfer, and of those 19 programmes, only one still involves unencrypted information being transferred.<sup>618</sup>

616 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 39.

617 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 45.

618 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 44.

- 9.13 It is because of the risks to privacy, the risks of adverse action being taken against individuals without justification, and the risk of undermining public trust and confidence in government, that the Privacy Act imposes controls on information matching. These controls are directed at:<sup>619</sup>
- authorisation – making sure that only programmes clearly justified in the public interest are approved;
  - operation – ensuring that programmes are operated consistently with fair information practices; and
  - evaluation – subjecting programmes to periodic reviews and possible cancellation.

### The basic framework

- 9.14 The Act controls information matching by providing:
- for its authorisation by statute (an “information matching provision” – these are set out in Schedule 3 of the Act);
  - that information matching programmes carried out by agencies (“specified agencies”, defined in section 97) must be done pursuant to information matching agreements that comply with certain rules; and
  - that certain procedural safeguards must be followed before action (“adverse action”, defined in section 97) is taken against an individual in reliance on the results of a matching programme.
- 9.15 If an information matching provision is in place authorising an information matching programme, the following requirements and safeguards apply:
- The specified agencies authorised to participate in the information matching programme must have in place an information matching agreement before they disclose or receive personal information for the purposes of the programme.<sup>620</sup>
  - The information matching agreement must incorporate provisions that reflect the information matching rules set out in Schedule 4 of the Act, or provisions that are no less onerous.<sup>621</sup> The information matching rules are discussed below.
  - The specified agencies must comply with the agreement,<sup>622</sup> and must supply a copy (and any subsequent amendments) to the Privacy Commissioner.<sup>623</sup>
  - The agencies involved in an information matching programme must take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it, unless to do so would be likely to frustrate the objective of the programme.<sup>624</sup>
  - If an information matching programme produces a “discrepancy”,<sup>625</sup> the agency must, within 60 working days, make a decision whether or not to take adverse action against an individual on the basis of that discrepancy. If no

619 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 40.

620 Privacy Act 1993, s 99(1).

621 Privacy Act 1993, s 99(2).

622 Privacy Act 1993, s 99(2).

623 Privacy Act 1993, s 99(4).

624 Privacy Act 1993, sch 4, r 1.

625 A discrepancy (defined in section 97) “in relation to an authorised information matching programme, means a result of that programme that warrants the taking of further action by any agency for the purpose of giving effect to the objective of the programme.”

decision to take adverse action is made within that period, the agency must destroy the information that disclosed the discrepancy.<sup>626</sup>

- The adverse action must be commenced within 12 months of obtaining the information that disclosed the discrepancy.<sup>627</sup>

9.16 Before an agency takes adverse action against an individual on the basis of a discrepancy, the agency must:

- notify the individual, in writing, of the particulars of the discrepancy and of the adverse action that it proposes to take;<sup>628</sup>
- tell the individual that he or she has five working days from receiving the notice to provide a good reason why the adverse action should not be taken,<sup>629</sup> and
- wait for those five working days to expire.<sup>630</sup>

In some cases, an agency can take adverse action against an individual without complying with the notice and delay requirements in section 103(1). There is a general exemption if compliance would prejudice any investigation into the commission of an offence or the possible commission of an offence.<sup>631</sup> In addition, there are specific exemptions for certain agencies in respect of certain information matching programmes.<sup>632</sup>

9.17 An agency to which personal information is disclosed for use in an information matching programme cannot keep the information indefinitely. If the information does not reveal a discrepancy, the agency must destroy that information as soon as practicable.<sup>633</sup> If the information reveals a discrepancy, the agency must destroy that information as soon as practicable after the information is no longer needed for the purposes of taking any adverse action against any individual.<sup>634</sup>

9.18 Likewise, an agency that holds information produced by an information matching programme cannot keep the information indefinitely. The agency must destroy the information:

- if the agency becomes aware of a discrepancy as a result of the information, and the agency has not made a decision to take adverse action against any individual on the basis of the discrepancy within 60 working days of becoming aware of the discrepancy;<sup>635</sup> or
- as soon as practicable after the agency decides not to take adverse action against any individual on the basis of the information;<sup>636</sup> or
- as soon as practicable after the information is no longer needed for the purposes of taking adverse action against any individual.<sup>637</sup>

626 Privacy Act 1993, s 101(1).

627 Privacy Act 1993, s 101(2).

628 Privacy Act 1993, s 103(1)(a)(i).

629 Privacy Act 1993, s 103(1)(a)(ii).

630 Privacy Act 1993, s 103(1)(a)(ii).

631 Privacy Act 1993, s 103(2).

632 Privacy Act 1993, ss 103(1A), (1B), (2A); Corrections Act 2004, s 180C.

633 Privacy Act 1993, sch 4, r 6(1).

634 Privacy Act 1993, sch 4, r 6(2).

635 Privacy Act 1993, s 101(1).

636 Privacy Act 1993, s 101(3).

637 Privacy Act 1993, s 101(4).

- 9.19 The Inland Revenue Department (IRD) is exempt from the requirements in section 101 and rule 6. We comment on the justification for this exemption later in the chapter.
- 9.20 The Privacy Commissioner can extend the time limit set out in section 101 in respect of information produced by an information matching programme if satisfied that an agency cannot reasonably be required to meet it, for example because of the amount of the information or the complexity of the issues involved.<sup>638</sup>
- 9.21 A failure to comply with the provisions of Part 10 in relation to an individual is an action that is an interference with the privacy of that individual,<sup>639</sup> and can therefore be the subject of a complaint to the Privacy Commissioner under section 67.
- 9.22 The Act imposes a number of detailed reporting requirements with respect to information matching programmes, as follows:
- Whenever required by the Privacy Commissioner, the agencies involved in a programme must provide the Commissioner with a report setting out whatever details the Commissioner requires.<sup>640</sup>
  - The Privacy Commissioner's annual report must include a report on each information matching programme carried out during the year to which the annual report relates.<sup>641</sup>
- 9.23 The Act also provides for authorised information matching programmes to be subject to periodic evaluation.<sup>642</sup> The Privacy Commissioner is required to review the operation of every information matching provision at intervals of not more than five years, consider whether or not the authority conferred by the provision should be continued or whether any amendments to the provision are necessary or desirable, and report his or her findings to the responsible Minister.<sup>643</sup>
- 9.24 The Privacy Commissioner also has a function of examining and reporting on proposed legislation where the Commissioner considers that personal information authorised to be collected or disclosed by a public sector agency under the proposed legislation might be used for the purpose of an information matching programme.<sup>644</sup> In the course of that examination, the Commissioner is to have particular regard to the matters set out in section 98.
- 9.25 A special information matching regime is provided for under the Social Welfare (Transitional Provisions) Act 1990. This provides for the exchange of information between New Zealand and other countries under reciprocal social security agreements or conventions. The special regime is examined in more detail below.

---

638 Privacy Act 1993, s 102.

639 Privacy Act 1993, s 66(1)(a)(iii).

640 Privacy Act 1993, s 104.

641 Privacy Act 1993, s 105.

642 Privacy Act 1993, s 106.

643 Privacy Act 1993, s 106.

644 Privacy Act 1993, s 13(1)(f).

### The information matching rules in Schedule 4

- 9.26 The information matching rules are set out in Schedule 4 of the Act. They are based to a large extent on the provisions of the Australian federal Data-matching Program (Assistance and Tax) Act 1990.<sup>645</sup>
- 9.27 The information matching rules are a mixture of general and detailed technical requirements. The key provisions of the information matching rules are as follows:
- Agencies involved in an information matching programme must take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it, unless that would be likely to frustrate the objective of the programme (*rule 1*).
  - Unique identifiers cannot be used as part of an information matching programme, unless their use is essential in the success of the programme (*rule 2*).
  - Online computer connections must not be used to transfer information between agencies for the purposes of an information matching programme, unless the Privacy Commissioner approves the transfer (*rule 3*).
  - The agency primarily responsible for the operation of an information matching programme must establish and maintain detailed technical standards governing the operation of the programme. These standards must deal with certain matters set out in the rules (such as how the integrity of the information to be used in the programme, and the integrity of the programme itself, are to be maintained, and the security features included within the programme), and be incorporated in a Technical Standards Report. Compliance with the requirements set out in a Technical Standards Report is mandatory for all agencies involved in the relevant information matching programme (*rule 4*).
  - Agencies involved in information matching programmes must have reasonable procedures for confirming the validity of discrepancies before seeking to rely on them as the basis for action in respect of an individual, unless there are reasonable grounds to believe that the results are unlikely to be in error (*rule 5*).
  - Personal information disclosed for use in an information matching programme and that does not reveal a discrepancy must be destroyed as soon as practicable, and personal information that does reveal a discrepancy must be destroyed as soon as practicable after it is no longer needed for the purposes of taking any adverse action (*rule 6*).
  - Information used in information matching programmes must not be linked or merged to create a new separate register or databank of information about the individuals to whom the information relates (*rule 7*).
  - Yearly limits on the number of times matching is carried out under a programme must be established for programmes that are to last longer than a year or indefinitely (*rule 8*).

<sup>645</sup> This Act is examined in more detail below at paragraphs 9.73–9.75.

- 9.28 Section 107 of the Privacy Act authorises the amendment of the information matching rules by Order in Council. Amendments cannot be made otherwise than in accordance with recommendations of the Privacy Commissioner. Section 107 states that amendments can be made for the purposes of Part 10, but there is no other statement of the scope of section 107.
- 9.29 The power in section 107 has never been exercised. However, the Privacy Commissioner issued special reports in 2001<sup>646</sup> and 2003<sup>647</sup> recommending replacement of the information matching rules. These recommendations followed on from and built on the Commissioner's recommendations in *Necessary and Desirable*.

### Information matching programmes

- 9.30 The 2009 Annual Report of the Privacy Commissioner indicates that there are currently 50 active information matching programmes in place,<sup>648</sup> up from 46 in 2008.<sup>649</sup> In the 2008/2009 reporting year the Office of the Privacy Commissioner provided assistance on or commented on one new authorisation, the start of six new matches, and numerous changes to the scope and conditions of existing agreements.<sup>650</sup> During the same period, Parliament passed five new matching authorisations, all of which involved amendments to the Births, Deaths, Marriages and Relationships Registration Act 1995.<sup>651</sup>
- 9.31 The Passport Eligibility Programme authorised by section 78A of the Births, Deaths, Marriages, and Relationships Registration Act 1995 is a simple example of an information matching programme. The purpose of the programme is to assist in determining whether or not a person is eligible for a New Zealand passport, and to detect fraudulent applications. Identity information on passport applications is matched against births, deaths, and marriages registers. A match with an entry in the births and marriages registers means that the processing of the application can continue. A match with an entry on the deaths register halts the processing of the application so that a possible case of fraud can be investigated.<sup>652</sup>

---

646 Office of the Privacy Commissioner *Amendment of Information Matching rules. Report by the Privacy Commissioner to the Minister of Justice recommending that making of an Order in Council to revoke the Fourth Schedule to Privacy Act 1993 and to substitute a new Schedule containing a revised set of information matching rules* (Wellington, June 2001).

647 Office of the Privacy Commissioner *Amendment of Information Matching Rules: supplementary report. Report by the Privacy Commissioner to the Minister of Justice making supplementary recommendations to those contained in a report of 28 June 2001 recommending the replacement of the information matching rules by Order in Council* (Wellington, August 2003).

648 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

649 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 46.

650 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

651 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 42.

652 For more on this programme see Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 50.

### Matching that is outside Part 10

- 9.32 Part 10 does not control all information matching. To the extent that particular information matching would not otherwise be permitted by the privacy principles, an information matching provision specified in Schedule 3 provides the authority to undertake information matching in compliance with Part 10.
- 9.33 Section 108 provides that, where the collection or disclosure of information is authorised by an information matching provision, the maintenance of the law exceptions in privacy principles 2 and 11 cannot be used to avoid the controls on information matching in the Act. Equally, section 109 provides that agencies cannot use the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987 to exchange information and thereby avoid the controls on information matching.<sup>653</sup>
- 9.34 However, except where sections 108 and 109 apply, Part 10 does not apply where an agency is able to carry out information matching without reliance on the authority of an information matching provision. The Privacy Commissioner, in *Necessary and Desirable*, identified situations where this might be possible:<sup>654</sup>
- if the matching is authorised, either generally or specifically, by a statutory provision that is not listed as an information matching provision in Schedule 3;
  - if the matching is able to be carried out consistently with the privacy principles; or
  - if the matching is authorised by the Privacy Commissioner under section 54 of the Act, or by a code of practice.
- 9.35 The limited application of section 108 also raises the possibility that, even though an information matching provision is specified in Schedule 3, an agency could collect, disclose, and use personal information for the purposes of a matching programme in compliance with the privacy principles without relying on the maintenance of the law exception to principles 2 and 11. The agency would then effectively have a choice as to whether it complied with Part 10 or not.<sup>655</sup> Later in this chapter we explain our dissatisfaction with this position.

#### INFORMATION MATCHING UNDER THE SOCIAL WELFARE (TRANSITIONAL PROVISIONS) ACT 1990

- 9.36 Sections 19 to 19D of the Social Welfare (Transitional Provisions) Act 1990 enact a framework under which legal effect in New Zealand can be given to agreements or conventions between the New Zealand Government and the governments of other countries providing for mutual assistance in recovering social security debts and supplying information for social security purposes. Legal effect is given to an agreement by the making of an Order in Council that declares that certain provisions of the agreement or convention have the force of law in New Zealand, and that certain New Zealand enactments (such as the Social Security Act 1964) have effect subject to such modifications as may be required for the purpose of giving effect to the agreement or convention.

<sup>653</sup> Privacy Act 1993, s 109.

<sup>654</sup> See *Necessary and Desirable*, para 10.1.14.

<sup>655</sup> For a discussion of the “choice of power” situation and the legal principles that might apply, see further Christopher Enright *Federal Administrative Law* (Federation Press, Sydney, 2001) 83.

- 9.37 The Act sets out certain preconditions that must be complied with before an Order in Council can be made. If an agreement or convention contains provision for mutual assistance between the parties in the recovery of social security debts or for the supply of information, an Order in Council cannot be made unless the Privacy Commissioner has first reported to the Minister responsible for the administration of the Act and the Minister of Justice.<sup>656</sup> The report must consider whether or not the provision in the agreement or convention complies with the privacy principles (having regard to the information matching guidelines set out in section 98 of the Privacy Act),<sup>657</sup> and if the provision provides for the exchange of information between the parties, the adequacy of the other country's privacy protection for personal information that may be supplied by New Zealand.<sup>658</sup>
- 9.38 A provision in an agreement or convention providing for the exchange of information must be subject to a number of terms and conditions set out in section 19C of the Social Welfare (Transitional Provisions) Act, or terms and conditions to the same effect. Those terms and conditions include a requirement that any exchange of personal information be made only for social security purposes (although information supplied may be passed on to taxation authorities for tax assessment and enforcement purposes).<sup>659</sup> Any exchange of information must be made in accordance with an agreement between the relevant organisations in each country,<sup>660</sup> and, in relation to New Zealand, the agreement must be approved by the Privacy Commissioner,<sup>661</sup> contain the safeguards that must be included in an information matching agreement under the Privacy Act,<sup>662</sup> and require the information matching rules to be applied.<sup>663</sup> Information supplied to a country under the agreement or convention must also be subject to the same privacy protections as other personal information obtained under that country's social security laws.<sup>664</sup>
- 9.39 If information is supplied to the relevant New Zealand authority under a provision of an agreement or convention, section 19D(3) of the Act imposes procedural requirements that are similar to those in section 103 of the Privacy Act before the information can be used to take action against an individual. In addition, sections 100 to 102 and 104 to 106 of the Privacy Act apply in respect of the provision as if the provision were an authorised information matching programme. The oversight and reporting functions of the Privacy Commissioner therefore apply to the activities carried out under the provision.

656 Social Welfare (Transitional Provisions) Act 1990, s 19(2A). See, for example, Office of the Privacy Commissioner *Exchange of Social Security Information with the Netherlands: Report by the Privacy Commissioner to the Minister of Justice and the Minister of Social Development and Employment pursuant to section 19(2A) of the Social Welfare (Transitional Provisions) Act 1990 in relation to mutual assistance provisions in the revised reciprocity agreement on social security between New Zealand and the Netherlands* (Wellington, 2003). Available at [www.privacy.org.nz/exchange-of-social-security-information-with-the-netherlands](http://www.privacy.org.nz/exchange-of-social-security-information-with-the-netherlands).

657 Social Welfare (Transitional Provisions) Act 1990, s 19(2A)(a).

658 Social Welfare (Transitional Provisions) Act 1990, s 19(2A)(b).

659 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(a).

660 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d).

661 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(v).

662 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(iii).

663 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(d)(iv).

664 Social Welfare (Transitional Provisions) Act 1990, s 19C(1)(e).

- 9.40 Six active information matching programmes are currently carried out under two separate reciprocity agreements in place under section 19 of the Social Welfare (Transitional Provisions) Act 1990. Two programmes operate under an agreement between New Zealand and Australia, and four operate under an agreement between New Zealand and the Netherlands.<sup>665</sup> The operation of all six active information matching programmes is audited each year by the Privacy Commissioner. The 2009 Annual Report of the Privacy Commissioner indicates satisfaction that the programmes were generally conducted in accordance with applicable statutory requirements.<sup>666</sup>

OVERSIGHT OF  
INFORMATION  
MATCHING  
PROGRAMMES  
BY THE  
PRIVACY  
COMMISSIONER

Levels of oversight

- 9.41 The Privacy Commissioner performs an oversight role in relation to information matching at three levels. First, the Commissioner considers and reports on new proposals to authorise information matching under sections 13(1)(f) and 98 of the Privacy Act 1993 and section 19A of the Social Welfare (Transitional Provisions) Act 1990. Secondly, the Commissioner monitors and reports on authorised information matching programmes in accordance with Part 10 of the Privacy Act 1993 (including where this Part is applied by section 19D(3)(e) of the Social Welfare (Transitional Provisions) Act 1990). Thirdly, the Commissioner is required to undertake periodic reviews of the statutory authorities for information matching under section 106.

*Reporting on proposed authorisations for information matching*

- 9.42 The first function of considering and reporting on proposed information matching authorisations requires little comment. The function is part of a wider governmental and legislative process that seeks to ensure that new proposals to authorise information matching are justifiable, well scoped, and well designed. In *Necessary and Desirable*, the Privacy Commissioner found the process to be working satisfactorily, and made a small number of recommendations for minor improvements.<sup>667</sup> These related to the information matching guidelines set out in section 98 of the Privacy Act.
- 9.43 As part of the process of considering a legislative proposal for an information matching programme, the Privacy Commissioner requires the relevant agency to prepare an Information Matching Privacy Impact Assessment (IMPIA) report, describing the programme and its objectives, and how it will comply with the Privacy Act 1993. A detailed analysis of the proposal against the information matching guidelines set out in section 98 of the Privacy Act is a key part of the IMPIA. A guidance note for agencies seeking legislative provision for information matching has been prepared by the Privacy Commissioner and is available on the Privacy Commissioner's website.<sup>668</sup>

665 See "Data Matching – Operating Programmes" [www.privacy.org.nz/operating-programmes](http://www.privacy.org.nz/operating-programmes) (accessed 15 February 2010).

666 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, November 2009) 69, 77–79.

667 *Necessary and Desirable*, recommendations 122–124.

668 Office of the Privacy Commissioner *Guidance Note for Departments Seeking Legislative Provision for Information Matching* (Wellington, 2008). Available online at [www.privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching](http://www.privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching).

- 9.44 We discuss below the suggestion that this process be further enhanced by imposing a legislative requirement for agencies to prepare a written assessment of a proposed information matching programme in the form of a “programme protocol”.<sup>669</sup>

#### *Monitoring and reporting on information matching programmes*

- 9.45 The monitoring and reporting functions of the Privacy Commissioner in relation to information matching programmes constitute a major activity for the Commissioner and her staff. Section 105 of the Privacy Act requires that the Commissioner report each year on the information matching programmes carried out during that year, and include an assessment of the extent of each programme’s compliance with sections 99 to 103 of the Act and the information matching rules. The work involves a significant resource commitment on the part of the Commissioner. Two fulltime resources within what is a small office are devoted to information matching. The 2009 Annual Report of the Commissioner reports on 50 programmes, and this constitutes close to a third of the Commissioner’s report.
- 9.46 The Privacy Commissioner’s oversight of an information matching programme does result in the identification of issues that the relevant agency needs to address. The Commissioner’s 2009 Annual Report indicates that all but one<sup>670</sup> of the 50 operative programmes were generally operated in compliance with the Privacy Act (and, where applicable, the Social Welfare (Transitional Provisions) Act 1990), although in two cases she identified technical issues with programmes,<sup>671</sup> and in one other case identified issues with the agencies’ retention and verification practices.<sup>672</sup> In her 2007 Annual Report, the Privacy Commissioner raised concerns about the quality of the matching results being acted upon in the Customs/Justice Fines Defaulters Alert Match, and indicated that on the basis of those concerns she could not confirm that the programme was being conducted in compliance with the Act.<sup>673</sup> As a result of those concerns, an inter-agency project team was established to review of the operation of this match (in conjunction with the Office of the Privacy Commissioner). The Commissioner’s 2008 Annual Report indicated satisfaction with the operation of the programme, while noting that the review had highlighted a number of procedural arrangements that could be improved and that were in the process of being implemented.<sup>674</sup> The 2009 Annual Report shows that this matching programme is compliant with the requirements under the Act.<sup>675</sup>

---

669 See below paragraphs 9.128–9.131.

670 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2009) 65.

671 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 58, 63.

672 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 64–65.

673 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2007* (Wellington, 2007) 95.

674 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 107–108.

675 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 60.

*Review of information matching authorities*

- 9.47 The third function of the Privacy Commissioner in relation to information matching is to review the statutory authorities for information matching at intervals of not more than five years in accordance with section 106 of the Privacy Act. In carrying out a review, the Commissioner must consider whether or not the authority should be continued, and whether any amendments to the relevant statutory provision are necessary or desirable, and report his or her findings to the responsible Minister.
- 9.48 The Privacy Commissioner has published the results of two reviews carried out under section 106.<sup>676</sup> The first was published in May 1999, and reviewed authorities to carry out two information matching programmes under the Customs and Excise Act 1996 and the Tax Administration Act 1994. The second was published in May 2002, and reviewed authorities to carry out four information matching programmes under the Penal Institutions Act 1954, the Tax Administration Act 1994, and the Immigration Act 1987. Section 106 of the Privacy Act does not prescribe the considerations that the Commissioner should take into account in undertaking a review, but the Commissioner indicated in both reviews that the information matching guidelines set out in section 98 of the Act are a major basis of that consideration.
- 9.49 Of the six authorities for information matching reviewed by the Privacy Commissioner, the Commissioner has recommended that five be continued and one be repealed (the NZIS/MSD Immigration match under the Immigration Act 1987, on the basis that the authority was not being utilised).<sup>677</sup> In relation to one authority, the Commissioner recommended the repeal of a related provision of the Privacy Act (section 103(1A)).<sup>678</sup> None of these recommendations have been implemented. There is no requirement in section 106 of the Privacy Act for the Government to respond to any recommendations in a Commissioner's report under that section.
- 9.50 No further reports on section 106 reviews have been published. The 2004 Annual Report of the Privacy Commissioner indicated that the objective of completing section 106 reviews of a further three information matching programmes had not been achieved due to demands on limited resources.<sup>679</sup> The 2008 Annual Report of the Privacy Commissioner indicated that the Commissioner is currently carrying out a section 106 review of one of the information matching programmes carried out under section 84 of the Tax Administration Act 1994, but no timeframe was outlined.<sup>680</sup> At the date of writing, this review has not been finalised.

---

676 Both are available online at [www.privacy.org.nz/information-matching-reports-and-reviews](http://www.privacy.org.nz/information-matching-reports-and-reviews).

677 Office of the Privacy Commissioner *Review of statutory authorities for information matching (Second Report)* (Wellington, May 2002) 31.

678 Office of the Privacy Commissioner *Review of statutory authorities for information matching* (Wellington, May 1999) 7.

679 Office of the Privacy Commissioner *Annual Report of the Privacy Commissioner for the year ended 30 June 2004* (Wellington, November 2004) 111.

680 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, November 2008) 92.

- 9.51 The review of authorising provisions for information matching is an important part of the overall system of oversight of information matching. Since these authorising provisions constitute an exception to the privacy principles, it is appropriate that each authority is regularly reviewed to establish whether or not it is still needed, whether or not the expected benefits from the programme are (still) being realised and are sufficient to justify the inroads into privacy that the programme involves, and whether or not the actual operation of the programme over the review period provides sufficient confidence that the risks to privacy arising from the programme have been sufficiently well-managed to justify the continued existence of the programme. Indeed, the section 106 review procedure was included in the Act, as an adjunct to the requirement that all information matching programmes be authorised by statute, in the place of the procedure originally proposed in the Privacy of Information Bill as introduced. Under that procedure, in addition to certain statutorily authorised information matching programmes, the Privacy Commissioner would have been empowered to issue both permanent and time-limited information matching approvals. The Commissioner would also have been empowered to revoke any such approval on the grounds that it no longer met the requirements for approval or for non-compliance with the conditions of the approval or the information matching rules.
- 9.52 Resourcing constraints have prevented both the current and the previous Privacy Commissioner from undertaking the regular reviews of information matching authorities required by section 106. We make some suggestions about this below.<sup>681</sup>

### Report on an unauthorised information matching programme

- 9.53 There is one reported case of information matching not authorised by statute (that is, it had not been listed as an “authorised information matching programme” subject to Part 10 of the Act) being undertaken by a New Zealand government agency. In 2000, the Privacy Commissioner investigated information matching undertaken in 1998 by the Department for Courts.<sup>682</sup> The programme matched the Department’s list of fines defaulters against personal details on the motor vehicle register in order to obtain updated address information.
- 9.54 Significant data quality problems with the programme meant that many of the people who were identified in the data match, and who were subsequently sent letters requiring them to repay fines promptly, were not the individuals who owed the fines. While the further particulars of the incident need not be considered here, in his report the then Privacy Commissioner stated:<sup>683</sup>

I am extremely concerned about departments seeking to undertake data matching which has not been authorised through Part X of the Act. It is quite at variance with the Government policy lying behind the establishment of Part X. It makes little sense that Cabinet should authorise some public sector data matching subject to strict controls while officials take it upon themselves to initiate other significant matching totally

<sup>681</sup> See paragraphs 9.138–9.141 below.

<sup>682</sup> Office of the Privacy Commissioner *Unauthorised information matching between Department for Courts and motor vehicle register: Report to the Ministers of Justice, Courts and Transport in relation to an inquiry into events surrounding unauthorised information matching programme operated in mid-1998* (Wellington, 2000).

<sup>683</sup> Office of the Privacy Commissioner *Unauthorised information matching between Department for Courts and motor vehicle register: Report to the Ministers of Justice, Courts and Transport in relation to an inquiry into events surrounding unauthorised information matching programme operated in mid-1998* (Wellington, 2000) 2.

unregulated by Part X. If public confidence is to be maintained in the fair handling of public sector information and in the responsible use of data matching, it is critical that departments go through the rigorous process of justification and assessment in establishing a programme and that the practice be authorised at the highest level.

### Other activities

9.55 In addition to the three specific oversight functions conferred on the Privacy Commissioner by the Act, the Commissioner and her staff devote considerable resources towards informing and educating government agencies involved in information matching. The Commissioner holds meetings of agencies involved with or interested in information matching. Training workshops are held for people who are or may be involved in developing an authorised information matching programme. An Information Matching Bulletin containing information and articles on information matching is published periodically.<sup>684</sup> A *Guidance Note for Departments Seeking Legislative Provision for Information Matching* has been produced along with a resource document about the information matching guidelines,<sup>685</sup> and draft Guidance notes for online transfer approvals have also been distributed for feedback and comment.<sup>686</sup> In addition, for the last few years, an *Information Matching Compliance Auditing Information Pack* has been made available each year to agencies involved in information matching.<sup>687</sup> The pack provides the government agencies with audit templates and guidance material to enable them to provide the statutorily required reports to the Privacy Commissioner on their information matching programmes.

#### CHANGES IN INFORMATION MATCHING SINCE 1991

9.56 There have been significant changes in the extent and nature of information matching since the enactment of the original information matching controls in the Privacy Commissioner Act 1991. Societal, international, and technological changes have also had an impact. The following are the key changes in information matching since 1991:

- The number of agencies involved has grown significantly. In 1991, eight separate enactments provided 10 individual statutory authorisations<sup>688</sup> for information matching involving eight separate agencies. As at September 2009, 16 separate enactments provide over 40 individual statutory authorisations for information matching involving at least 24 separate agencies (including generic classes of agency such as institutions and private training establishments within the meaning of section 159 of the Education Act 1989). The Privacy Commissioner reports that, between 1998 and 2008, the number of agencies from which data for information matching programmes is sourced has doubled, and the number of agencies that use this source data has more than doubled.<sup>689</sup>
- The number of active information matching programmes has increased

684 Three editions were published during the 2008/2009 reporting year. Available online at [www.privacy.org.nz/information-matching-bulletins](http://www.privacy.org.nz/information-matching-bulletins).

685 Office of the Privacy Commissioner *Guidance Note for Departments Seeking Legislative Provision for Information Matching* (Wellington, May 2008).

686 Available online at [www.privacy.org.nz/resources-for-government-agencies](http://www.privacy.org.nz/resources-for-government-agencies) (accessed 13 January 2010).

687 Office of the Privacy Commissioner *Information Matching Compliance Auditing Information Pack* (Wellington, 2009).

688 These are the information matching provisions that were listed in Schedule 3 of the Privacy Commissioner Act 1991.

689 Office of the Privacy Commissioner *Information Matching Bulletin* (December 2008) 2.

significantly. The Privacy Commissioner reports that, between 1998 and 2008, the number increased from 12 to 46 (out of a total of 80 authorised information matching programmes).<sup>690</sup> This number increased to 50 in 2009.

- The purposes for which information matching is carried out have evolved, with a shift towards purposes that are more beneficial to individuals than the original focus on detecting and avoiding benefit fraud. The Privacy Commissioner has compared the purposes of the information matching programmes carried out in 1997/98 with those carried out in 2007/08. Over 75 per cent of the matching programmes carried out in 1997/98 were to confirm eligibility for a benefit or to detect illegal behaviour. In 2007/08, only just over 50 per cent of information matching programmes were carried out for those purposes. Purposes that had assumed greater significance included locating people, updating data, and identifying unclaimed entitlements.<sup>691</sup>
- A huge increase in the amount of personal information that is held in computerised form and massive advances in information technology have significantly increased the ability of agencies to undertake information matching. Not only does this increase the scale of information matching that is possible,<sup>692</sup> it is now also economic to undertake much smaller matches than previously. However, as information systems technology has evolved, concerns have been expressed that data quality problems have increased as well. One commentator has suggested that this is the result of rapid systems development that has made quality hard to control, and that standards, techniques, methods, and tools for managing quality have evolved at a slower pace than the systems they support.<sup>693</sup>
- Information matching was originally carried out through the transfer of data on computer tape or disk. The information matching rules prohibit online matching without the approval of the Privacy Commissioner. In *Necessary and Desirable*, the then Privacy Commissioner reported that he had granted such an approval in respect of one information matching programme. The Privacy Commissioner's 2009 Annual Report indicates that over half (26) of the 50 active programmes have approvals to undertake online matching.<sup>694</sup>
- The original information matching programmes involved data generated and matched domestically. Some information matching programmes now involve the transfer of data to another jurisdiction, or receipt of data from another jurisdiction. Social security mutual assistance schemes authorised under the Social Welfare (Transitional Provisions) Act 1990 are an example.
- The initial authorised information matching involved core government agencies such as the Department of Social Welfare and the IRD. A broader range of

---

690 Office of the Privacy Commissioner *Information Matching Bulletin* (December 2008) 2.

691 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2008* (Wellington, 2008) 46–47.

692 For example, in the year to 30 June 2007, the Department of Social Development's National Data Match Centre compared more than 12 million records with other agencies. This resulted in 193,358 matches and 18,588 cases of overpayments. The total value of these overpayments was \$19 million. See Office of the Auditor-General "Ministry of Social Development: Preventing, detecting, and investigating benefit fraud, performance audit report under section 16 of the Public Audit Act 2001" (Wellington, 2008) 31.

693 The commentator writes under the profile "Vijikumar" at <http://dataqualityaccuracy.blogspot.com>. See the articles "The Data Quality Problem", "Definition of Accurate Data", "Sources of Inaccurate Data", and "Implementing a Data Quality Assurance Program" published on that website on 13 December 2007. See also "Data quality accuracy dimension", a two-part article by Colin Trotter in the May and June 2008 *Information Matching Bulletins* published by the Office of the Privacy Commissioner, Wellington.

694 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 45.

government agencies are now involved in information matching, such as district health boards and the New Zealand Transport Agency. Private sector agencies now supply some of the information used in information matching, such as private training establishments under the Education Act 1989.

- Some of the procedural requirements imposed by Privacy Act as originally enacted have been overridden by subsequent legislative amendments for some information matching programmes. In five cases, the requirement in section 103 that people must be notified before adverse action is taken against them on the basis of the result of a match, and given an opportunity to challenge the proposed action, has been overridden.
- 9.57 Our overall conclusion from these developments is that the scale and importance of information matching in the operation of public sector agencies means that the controls and protections in the Privacy Act with respect to information matching are even more important now than when the Act was first enacted.

#### INFORMATION MATCHING AND DATA MINING

- 9.58 There is a close relationship between information matching and data mining. Indeed, information matching might be regarded as a specialised subset of data mining. Various definitions of data mining have been put forward. The Australian Law Reform Commission (ALRC) adopted a definition from the Ontario Information and Privacy Commissioner: “a set of automated techniques used to extract buried or previously unknown pieces of information from large databases”.<sup>695</sup> A more expansive definition was proffered by the US Government Accountability Office (GAO) in a 2004 report on data mining by federal agencies: “the application of database technology and techniques – such as statistical analysis and modelling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.”<sup>696</sup>
- 9.59 From the description of information matching above, it can be seen that both data mining and information matching employ modern technology to analyse a vast amount of previously inaccessible and unconnected information and to provide personal information about an individual. Both do so with various degrees of accuracy.
- 9.60 While information matching tends to be associated with public sector agencies, data mining spans both public and private sectors. Organisations in the private sector use it for such purposes as market research, design of sales or marketing campaigns, product development, customer relationship management, financial analysis, and fraud detection.

695 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 9.51.

696 United States Government Accountability Office *Data Mining: Federal Efforts Cover a Wide Range of Uses. Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate* (GAO-04-548, Washington D.C., May 2004). See also Government Accountability Office *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain* (GAO-05-866, Washington D.C. August 2005).

- 9.61 The 2004 GAO report indicates that US Federal agencies use data mining for a variety of purposes, such as improving service or performance, detecting fraud, waste and abuse, analyzing scientific and research information, managing human resources, detecting criminal activities or patterns, analysing intelligence and detecting terrorist activities.<sup>697</sup>
- 9.62 Concerns about data mining are very similar to those about information matching. The ALRC summarised these as follows:<sup>698</sup>
- Data mining is carried out without the data subject's knowledge or consent, and can reveal large amounts of previously unknown personal information about that individual. As a consequence, informing the individual about the collection and use of the information is difficult, and it is difficult for the individual to seek access to the information.
  - Data mining uses information collected for different purposes and in different contexts. The source information may have been inaccurate at the time of collection or may have become inaccurate subsequently. This raises doubts about the accuracy of the information derived from the data mining. The combination of information collected from different sources compounds the danger of inaccuracy.
  - Large amounts of personal information are collected and stored for the purpose of data mining, raising concerns about the security of the information. Note, however, that data mining can now be carried out without aggregating or homogenising the source information, which can be mined in many locations and in many formats.
- 9.63 The GAO has raised an additional concern about data mining: *function creep*.<sup>699</sup> The aggregation and organisation of large quantities of previously isolated pieces of information could tempt agencies to use the information for purposes beyond the scope originally specified when the information was collected.
- 9.64 Another US organisation, the Information Security and Privacy Advisory Board, produced a report in May 2009 recommending ways in which privacy law and policy might be updated in the light of technological change. It had this to say about data mining:<sup>700</sup>

Data mining techniques represent a fundamental change in the way the government accesses and uses data. In the past, the government collected and processed data on one person at a time [that is, with particularity], either in the course of administering a government program or where there was some suspicion that a person was engaged in fraud, criminal conduct, terrorism or intelligence activity. The government was authorised to keep this data for long periods of time, and to retrieve, share and analyse it for compatible purposes without serious controls. New techniques like data mining undermine these protections as the government analyses information en masse.

---

697 United States Government Accountability Office *Data Mining: Federal Efforts Cover a Wide Range of Uses. Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate* (GAO-04-548, Washington D.C., May 2004) ii.

698 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) paras 9.53–9.54.

699 United States Government Accountability Office *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks. Report to the Chairman, Committee on Appropriations, House of Representatives* (GAO-07-293, Washington D.C., February 2007) 19.

700 Information Security and Privacy Advisory Board *Toward A 21<sup>st</sup> Century Framework for Federal Government Privacy Policy* (Washington D.C., May 2009) 28.

- 9.65 In 2007 a Bill, the Federal Agency Data Mining Reporting Act 2007, was introduced into Congress.<sup>701</sup> It would not have imposed restrictions on data mining, but would have required the head of each department or agency of the Federal Government that engaged in any activity to use or develop data mining to submit an annual report to Congress on those activities. Data mining would have had a limited scope under the Act, essentially covering a programme involving pattern-based queries, searches, or other analyses of one or more electronic databases to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity. Excluded from the definition of “database” were telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.
- 9.66 The ALRC made no specific recommendations relating to data mining, although the scope of their recommended Unified Privacy Principles relating to collection, notification, data quality, use, and disclosure would clearly impose limitations on the activity.
- 9.67 A relatively recent phenomenon is the huge growth in the use of the internet for social interaction, and the willingness of people to post personal (and often very sensitive) information about themselves (and others) on social networking and other websites.<sup>702</sup> Whether through ignorance or choice, users often place no or very few limits on access to this information by others. This means that a rich vein of personal information is now available to be mined by both the public and private sectors. The technological capability to extract the personal information is matched only by the willingness of people to disclose it. A recent newspaper article on government monitoring of social networking websites reports the case of a woman convicted of social welfare fraud for claiming a benefit when she was in a relationship.<sup>703</sup> Her Facebook and Bebo profiles stated that she was living in a relationship with the father of her child, when she had told welfare authorities that she was single. The article indicates that a number of other New Zealand government agencies are using social networking websites as sources of information.<sup>704</sup>
- 9.68 To the extent that data mining is not information matching, the collection, disclosure, use, and unique identifier restrictions in the Privacy Act, and any specific authorising legislation, apply. The Privacy Act has specifically dealt with information matching by government agencies from the outset because of the particular privacy issues that it raises. Given that data mining raises similar issues, and the enormous scope for its use (and misuse) in relation to the vast amount of personal information now available online, it may now be time to consider greater controls.

701 Pub L 110-53, 121 Stat 266, s 804 (2007). The Bill never became law, as it lapsed at the end of the Congressional session.

702 For more on social networking see chapter 13.

703 “Big Brother Watching our Lives Online” (4 April 2009) *Dominion Post* A10–11.

704 See also “Brits Consider Tracking All UK Facebook Traffic” (18 March 2009) <http://news.zdnet.com> (accessed 15 February 2010). This article reported that the UK government was considering the surveillance and retention of all communications on social networking sites. The UK government subsequently dropped the idea: see *Home Office Protecting the Public in a Changing Communications Environment* (April 2009).

- 9.69 In a 2004 report for the State Services Commission on citizens' responses to E-government, the researchers noted that there was a widespread belief among participants in the survey that government will not misuse information they provide via the internet – whether that information relates to their work or personal lives.<sup>705</sup> However they also noted that:<sup>706</sup>

Confidence would be eroded if they found out that the government cross-matched data or extensively engaged in data mining—sharing data among departments and agencies and culling information from assorted databases to learn more about the public.

- 9.70 One possible starting point might be to require greater transparency and openness about data mining in New Zealand. A requirement on public agencies to report on their data mining activities, along the lines of the US legislation, is one option. We have an open mind on the issue. Public feedback on the level of concern about data mining, and how any concerns might be addressed, would be particularly valuable.

Q104 Should there be greater openness about data mining by public agencies? For example, should public agencies be required to report annually on their data mining activities?

## OVERSEAS APPROACHES TO INFORMATION MATCHING

- 9.71 In this section we examine the information matching regimes in Australia, Canada, the United Kingdom, the USA, and Hong Kong to see if they offer any insights or lessons for New Zealand.

### Australia

#### *Federal*

- 9.72 The Privacy Act 1988 (Cth) does not specifically regulate data matching, except in relation to the use of a tax-file number, but some of the Act's Privacy Principles may apply to the activity. National Privacy Principle 7.1, for instance, regulates the adoption and use by non-government entities of identifiers assigned by government entities.
- 9.73 The Data-matching Program (Assistance and Tax) Act 1990 provides authority for the transfer and matching of personal information between the Australian Taxation Office and certain other agencies. The provisions in Part 10 and Schedule 4 of the New Zealand Privacy Act were based closely on that Act. The purpose is to detect the overpayment of certain benefits, persons receiving duplicate benefits, and non-compliance with tax law obligations, as well as identifying people who are entitled to a benefit but not claiming it.

705 Rowena Cullen and Peter Hernon *Wired for Well-Being: Citizens' Response to e-government: A report presented to the E-government Unit, State Services Commission* (Wellington, 2004).

706 Rowena Cullen and Peter Hernon *Wired for Well-Being: Citizens' Response to e-government: A report presented to the E-government Unit, State Services Commission* (Wellington, 2004) 50.

- 9.74 The Act provides that agencies carrying out matching under the Act must comply with guidelines.<sup>707</sup> The latest guidelines issued by the Privacy Commissioner came into effect in 1997.
- 9.75 The effect of the Act and the guidelines is to set out what personal information can be used in data matching programmes, how data matching programmes are to be conducted, and how the results of a programme can be used. Procedural safeguards very similar to those applying under the New Zealand Act require individuals to be given a chance to dispute or explain the results of a matching programme before action is taken against them.
- 9.76 To provide guidance to agencies that carry out data-matching that is not covered by the 1990 Act, the Privacy Commissioner has issued voluntary data-matching guidelines.<sup>708</sup> Their aim is to ensure that data-matching programmes are designed and conducted in accordance with sound privacy practices and in a privacy-sensitive way.
- 9.77 The Guidelines also state that they aim to encourage a higher standard of regard for people's privacy rights in relation to data-matching than is required by bare compliance with the Information Privacy Principles.<sup>709</sup> In assessing compliance with the Information Privacy Principles, the Privacy Commissioner may take the guidelines into consideration, but non-adherence to the guidelines would not necessarily put an agency in breach of the Privacy Principles.
- 9.78 The ALRC considered suggestions that the voluntary data-matching guidelines applying to governmental agencies should be made mandatory, but rejected this on the basis that there is no indication that agencies are not currently complying with those guidelines.<sup>710</sup> It suggested that the Office of the Privacy Commissioner might review the adequacy of, and compliance with, the current guidelines if the Office considered this necessary.

### Victoria

- 9.79 We note that a different approach to the regulation of data matching in Australia is favoured by the Office of the Victorian Privacy Commissioner.<sup>711</sup> That Office undertook an audit of data-matching activities in state and local government in Victoria in 2005. In its report, the Office stated its attraction to the New Zealand generic statute model for regulating data matching, as combining openness, precision, and oversight.<sup>712</sup>

707 Data Matching Program (Assistance and Tax) Act 1990 (Cth), s 12.

708 Office of the Privacy Commissioner (Cth) *The use of data matching in Commonwealth administration – Guidelines* (Sydney, February 1998).

709 Office of the Privacy Commissioner (Cth) *The use of data matching in Commonwealth administration – Guidelines* (Sydney, February 1998) 3.

710 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, Wellington) para 10.97.

711 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, 2005).

712 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, 2005) 1.

- 9.80 In its submission to the ALRC review, the Office of the Victorian Privacy Commissioner reported its preference for a generic statutory regime.<sup>713</sup> In the absence of such a statute the Victorian OPC recently published a guide on data matching for the Victorian public sector.<sup>714</sup>

## Canada

- 9.81 In Canada, at the Federal level, the ability of agencies to collect, use, and disclose personal information for data matching purposes is generally governed by the requirements of the Privacy Act. At the detailed level, data matching is governed by a Treasury Board of Canada Secretariat Policy on Data Matching, published in 1989.<sup>715</sup> As a policy directive, it does not have the force of law. The policy requires that Federal agencies undertake a preliminary assessment of the feasibility of the proposed matching programme (including a cost-benefit analysis), and provide this assessment to the Privacy Commissioner at least 60 days before the programme begins to allow for an external review before it is implemented.
- 9.82 In a 2006 review of the Canadian Federal Privacy Act, the Canadian Privacy Commissioner reported that very few data matching proposals are reported to the Privacy Commissioner, and that the data matching policy was not well-known among agencies.<sup>716</sup> The Commissioner further indicated that data matching had long been a concern to that office, and that the Privacy Act lacked effective audit and control mechanisms on data matching.<sup>717</sup> Even though the Treasury Board data matching policy was to be revised, the Commissioner considered that legislative controls were required.<sup>718</sup>

## United Kingdom

- 9.83 The Data Protection Act 1998 applies generally to information matching in both the public and private sectors in the United Kingdom, but contains no specific provisions regulating it. The ability of agencies to undertake information matching therefore depends on whether or not this will comply with the Act's data protection principles and other requirements. Compliance tends to be subsumed under the question of whether or not the information required for the matching can legally be shared by the agencies involved. This involves, amongst other things, assessing whether the information sharing is necessary, whether the information to be shared is relevant and not excessive, and whether the information will be processed fairly. The Information Commissioner has also issued an Information Sharing Framework Code of Practice.<sup>719</sup>

---

713 Office of the Victorian Privacy Commissioner *Submission to the Australian Law Reform Commission's Review of Australian Privacy Law* (Melbourne, December 2007).

714 Office of the Victorian Privacy Commissioner *Data Matching in the Public Interest: A guide for the Victorian public sector* (Melbourne, 2009).

715 Treasury Board Secretariat *Policy on Data Matching* (1989), available online at [www.tbs-sct.gc.ca](http://www.tbs-sct.gc.ca) (accessed 15 February 2010).

716 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, 2006).

717 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, 2006).

718 Office of the Privacy Commissioner of Canada *Government Accountability for Personal Information: Reforming the Privacy Act* (Ottawa, June 2006).

719 Information Commissioner's Office *Framework Code of Practice for Sharing Personal Information* (London, 2007).

In addition, there are some specific legislative authorities for information matching in the UK. For example, the UK Audit Commission has powers under Part 2A of the Audit Commission Act 1998 to undertake data matching for the purpose of assisting in the prevention and detection of fraud.

### United States

9.84 The Office of Management and Budget (OMB) issued guidelines in 1979 in relation to computer matching at the Federal level. The guidelines were revised and reissued in 1982. The guidelines allowed computer matching to be undertaken under the “routine use” exemption to the Privacy Act 1974, and imposed controls such as a requirement for prior notification of a matching programme in the Federal Register setting out the benefits, costs, potential harm, and alternatives. Agencies were also to report on the match to the Director of the OMB, Speaker of the House, and President of the Senate. The guideline approach was not, however, a success. One commentator, Priscilla Regan, observes that “agencies did not follow the guidelines, the OMB did not monitor agencies’ activities, the public and interest groups did not respond to *Federal Register* notices, and there was little congressional reaction.”<sup>720</sup>

9.85 The Office of Technology Assessment (OTA), in 1986, produced a report on a survey of Federal agency use of electronic record systems. Regan summarises the findings of the survey as follows:<sup>721</sup>

The OTA concluded that the widespread use of computerised databases, electronic record searches and matches, and computer networking was rapidly leading to the creation of a de facto national database containing personal information on most Americans.

In response, the Computer Matching and Privacy Protection Act was enacted by Congress in 1988.<sup>722</sup> The Act amended the Privacy Act 1974, and further amendments were made in 1990.

9.86 The information matching provisions in the New Zealand Privacy Act are modelled closely on the US Act. Under the US Act, Federal agencies involved in computer matching programmes (principally those relating to eligibility for Federal benefit programmes)<sup>723</sup> must negotiate written agreements with the other agencies that are participating in the programme, and those agreements must be approved by a data integrity board (which each agency conducting or participating in a matching programme must establish). Matching agreements must specify the legal authority and purpose of the programme, the justification for the programme and the anticipated results (including an estimate of any savings), and how matching under the programme is to be carried out.<sup>724</sup>

720 Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (UNC Press, Chapel Hill, 1995) 87.

721 Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (UNC Press, Chapel Hill, 1995) 95.

722 5 USC § 552a (o) – (u).

723 There are wide exemptions for law enforcement, intelligence, and tax purposes.

724 5 USC. § 552a (o).

- 9.87 A Government Accountability Office review of the implementation of the Act in 1993 identified deficiencies.<sup>725</sup> Apparently the cost-benefit analysis required before a programme is approved was often inadequate, and the data integrity boards did not provide adequate supervision.<sup>726</sup> A 2008 Government Accountability Office report on computer matching by the Inland Revenue Service is still not particularly encouraging.<sup>727</sup>
- 9.88 It should be noted that in addition to the Privacy Act and the Computer Matching and Privacy Protection Act, Congress has enacted the E-Government Act 2002.<sup>728</sup> Among other things, the Act requires Federal departments and agencies to conduct privacy impact assessments (PIAs) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form, or before initiating any new electronic data collections containing personal information on 10 or more individuals. A new computer matching initiative may therefore trigger the need for a PIA under this Act. However, OMB guidance on the Act indicates that a PIA is not required when all elements of a PIA are addressed in a matching agreement governed by the Computer Matching and Privacy Protection Act.<sup>729</sup>

## Hong Kong

- 9.89 The Hong Kong Personal Data (Privacy) Ordinance, section 30, regulates data matching in Hong Kong. The Ordinance was enacted in 1995, but the data matching provisions did not come into force until August 1997. The Ordinance is overseen by the Privacy Commissioner for Personal Data. Unusually, the relevant provision of the Ordinance applies to data matching by the public and private sectors.<sup>730</sup> Data matching is defined as a comparison of two sets of personal data, each of which is collected for different purposes, where each comparison involves the personal data of 10 or more data subjects, the comparison is carried out using a computer programme designed and applied for performing the comparison process and not by manual means, and the end result of the comparison may be used, whether immediately or at any subsequent time, for the purpose of taking adverse action against any of the data subjects concerned. Data matching that does not fall within the definition could still be covered by the data protection principles and other provisions of the Ordinance.

725 Government Accountability Office *Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by the 1988 Act* (GAO/PEMD-94-12, October 1993).

726 See further, Roger Clarke “Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism” (1995), available online at [www.rogerclarke.com](http://www.rogerclarke.com).

727 Government Accountability Office *Tax Administration: IRS Needs to Strengthen Its Approach for Evaluating the SRFMI Data-Sharing Pilot Program; a report to the Committee on Finance, U.S. Senate* (GAO-09-45, November 2008).

728 44 USC § 101.

729 Office of Management and Budget *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Memorandum M-03-22, Washington, D.C., 26 September, 2003).

730 The Law Reform Commission of Hong Kong report that preceded the Ordinance expressed particular concerns about “investigative data matching” that could lead to an adverse decision against an individual. This could arise in both the public and private sectors, for example in insurance and credit reporting. Law Reform Commission of Hong Kong *Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27)* (Hong Kong, 1994) 121, 129–130.

- 9.90 A data user must not carry out a matching procedure unless all the individuals who are the subjects of the data to be matched have voluntarily given express consent to the matching procedure being carried out, or the Privacy Commissioner for Personal Data has consented to the matching procedure being carried out, or the matching procedure belongs to a class of permitted matching procedures gazetted by the Privacy Commissioner or is required or permitted by a specified law.<sup>731</sup>
- 9.91 The overwhelming majority of applications for the Privacy Commissioner's approval to a matching procedure appear to come from the public sector, and in relation to social security benefit, law enforcement, and tax matters. Very few applications for approvals or re-approvals appear to be refused, but conditions are often imposed.

RESTRICTIONS  
ON INFORMATION  
MATCHING STILL  
NEEDED

- 9.92 We noted earlier that one of the principal reasons why privacy legislation was enacted in the early 1990s was to authorise the exchange of information between certain government agencies for the purpose of combating fraud and abuse of the social welfare system, and subject those information exchanges to a system of controls, reporting and monitoring. As can be seen from our examination of subsequent developments, the scale and reach of information matching by government agencies has increased significantly since then.
- 9.93 The risks to individual privacy are consequently just as great, if not greater. As one commentator (albeit in the US context) has said: “the principle underlying the [Privacy Act 1974, (US)] – that individuals should be able to exercise control over information about themselves that they provide to the government – is a bedrock principle of individual privacy. That principle is at war with the practice of computer matching.”<sup>732</sup>
- 9.94 The modern state could not function effectively without access to the vast amount of personal information provided directly by citizens or collected in other ways. Increasingly sophisticated technology provides the tools to use that information for socially beneficial purposes, such as improving service delivery, the more efficient use of resources, the protection of government revenue, and research. These and other benefits of information matching need to be balanced with the risks to privacy. Striking the right balance can build and maintain citizens' trust in government, providing the assurance that citizens can continue to provide the state with the information it needs to function, confident that their information will be protected and used appropriately.

731 Personal Data (Privacy) Ordinance (Cap 486) (HK), s 30(1).

732 John Shattuck “Computer Matching is a Serious Threat to Individual Rights” (1984) 27 Communications of the ACM 538.

9.95 The issue is neatly summarised by the Victorian Office of Privacy Commissioner as follows:<sup>733</sup>

Addressing data matching is part of the larger challenge of ensuring that the collection and handling of personal information in a technological age is done according to longstanding values, including respect for privacy. In its Information Privacy Principles, Victoria has adopted well known international data protection standards. This is partly to build trust, partly to keep a check on potential abuse of power, and partly to ensure that the necessary data continues to be available. If people lack trust in authorities, or do not believe that abuses can be detected and checked, then they begin to act in self defence. They may provide false or incomplete data. This in turn reduces the quality of decisions based on the data. This is not in the public interest and, over time, it will corrode the legitimate tasks of public administration, for which personal information, aided by technology, is necessary.

9.96 We therefore have no doubt that controls on information matching by government agencies are still required and, subject to what we say below, we think the current controls appear to be working reasonably well. Based on the results of the Privacy Commissioner’s audit regime and reports, compliance by agencies with the statutory requirements is high. On that basis, we can find no case for substantial change.

9.97 The New Zealand regime also compares favourably with the overseas regimes we have examined. The “openness, precision, and oversight” features rated so highly by the Victorian Office of Privacy Commissioner are of key importance. New proposals to enact information matching authorities are the subject of rigorous evaluation and debate. In comparison with more general principles or guidelines, the detailed statutory regime provides greater certainty to agencies as to what they can and cannot do. In that respect, Part 10 and Schedule 4 are effectively a statutory code of practice with respect to information matching.

9.98 We also consider that the Privacy Commissioner’s oversight of information matching is appropriate, given the nature of information matching. Because of the remote connection between information matching programmes and the individuals whose data is matched, reliance on the normal individual complaint and enforcement mechanisms of the Privacy Act to curb or detect abuses is unlikely to be effective.

Q105 We consider that the current controls on information matching by public sector agencies are appropriate and should be retained. Do you agree?

733 Office of the Victorian Privacy Commissioner *Victorian Public Sector Data Matching Audit* (Melbourne, February 2005) 2.

OPTIONS AND  
PROPOSALS  
FOR CHANGE

Information matching and the private sector

- 9.99 The information matching provisions in the Privacy of Information Bill as introduced in 1991 applied to both the public and the private sector. The Bill as reported back by the Justice and Law Reform Select Committee limited the information matching provisions to the public sector, on the basis that information matching in the private sector could be regulated by code of practice if necessary.<sup>734</sup> This is reflected in section 46(4)(a), which provides that a code of practice may impose controls on information matching by agencies that are not public sector agencies.
- 9.100 In the absence of a code of practice, information matching in the private sector is therefore, for the most part, regulated by the privacy principles relating to the collection, use, and disclosure of personal information, and the use of unique identifiers.
- 9.101 The only code of practice that expressly addresses information matching in the private sector is the Credit Reporting Privacy Code 2004, rule 8(2) of which provides that:
- A credit reporter must, when undertaking a comparison of personal information with other personal information for the purpose of producing or verifying information about an identifiable individual, take such measures as are reasonably practicable to avoid the incorrect matching of the information.
- 9.102 By comparison with the detailed provisions of Part 10 and Schedule 4 of the Act, the code therefore leaves it very much to individual credit reporters to determine the reasonably practicable steps they must take to avoid incorrect matches. However, this must also be seen in the context of the restrictions on the kinds of personal information that credit reporters are lawfully able to collect, and therefore use for identity verification. Forms of unique identification such as a driver's licence cannot be used for this purpose.
- 9.103 Are there differences between public and private sector agencies in terms of how they collect, use, and disclose personal information, and the privacy risks arising therefrom, that justify different treatment in terms of restrictions on information matching? Public sector agencies will often have the power to compel people to provide personal information, whereas private sector agencies can usually collect information only by consent. However, in a number of situations an individual's ability not to provide information to an agency is not determined by whether the agency is public or and private. A person's choice is very limited when it comes to basic services provided by the private sector such as energy, telecommunications, and banking, and the terms of service tend to be the same for all providers. To obtain the service, the individual will usually have to provide the personal information requested by the provider, and agree to the terms and conditions that the provider specifies with respect to how that information may subsequently be used.

<sup>734</sup> H Hancock (18 March 1993) 533 NZPD 14133.

- 9.104 Nevertheless, we are not in a position to say that there are sufficiently widespread and serious problems with the use of information matching by the private sector that restrictions similar to Part 10 and Schedule 4 should be extended to that sector. The Privacy Commissioner has not recommended it, nor has the Commissioner made or proposed any general or specific code of practice with respect to it (apart from the Credit Reporting Privacy Code). We need further information on this issue before coming to any firm conclusion, and welcome submissions on the point.
- 9.105 There are also options short of regulation that might be considered. One of these options is the issuing of guidelines by the Privacy Commissioner. Such guidelines would not be binding, but the Privacy Commissioner could take them into account in assessing compliance with the privacy principles.
- 9.106 Our proposal in chapter 6 to confer an audit power on the Privacy Commissioner is also relevant here. An appropriate audit power would enable the Privacy Commissioner to investigate current practices with respect to information matching in the private sector to see if any action is required.

Q106 We do not think that there is currently a case to impose detailed controls on information matching by private sector agencies. Do you agree? If not, can you provide examples of situations where a lack of controls has put people's privacy at risk?

### A separate Data Matching Act

- 9.107 In *Necessary and Desirable* the Privacy Commissioner described Part 10 as “relatively technical.”<sup>735</sup> We think this significantly understates its specialised, complex, and arcane nature. Further, unlike the rest of the Act (with the exception of Part 11 and Schedule 5, which deal with law enforcement information), Part 10 and Schedule 4 relate only to public sector agencies.
- 9.108 We consider that the technical, complex, and restricted nature of Part 10 means that it is out of place in a general information privacy statute. Most users of the Act will never need to refer to it, and it therefore clutters up the Act. On the other hand, Part 10 contains important privacy protections that justify statutory recognition. We therefore propose that Part 10 and Schedule 4 should not be included in a new Privacy Act but (as in Australia) enacted as a separate Act, along with the detailed changes we propose below. The new Act might be called the Privacy (Public Sector Data Matching) Act.
- 9.109 Even if Part 10 and Schedule 4 are enacted as a separate Act, it will be important to emphasise the new Act's privacy protection aspects and its continuing connection with the Privacy Act. This can be achieved through the inclusion of a purpose provision and appropriate cross-references between each Act.

---

<sup>735</sup> *Necessary and Desirable* para 10.1.3.

Q107 We propose that Part 10 and Schedule 4 should be enacted as a separate Privacy (Public Sector Data Matching) Act. Do you agree?

### Detailed changes

9.110 We think that a number of changes to Part 10 are necessary to clarify, modernise, and simplify its provisions. These go beyond just updating the structure, drafting style, and format, and introducing useful aids to clarity (such as a flowchart of the information matching process). A number of detailed recommendations have been made by the Privacy Commissioner in *Necessary and Desirable* and subsequent supplementary reports. Where appropriate, these recommendations are included here.

### Widen scope

9.111 We noted above that Part 10 does not currently regulate all information matching by public sector agencies.<sup>736</sup> Except in certain limited circumstances, even where a specific statutory authority to undertake information matching exists, a public sector agency does not have to utilise that authority and comply with Part 10 if it can rely on an alternative source of authority (such as the privacy principles and their exceptions). There are “anti-avoidance” mechanisms in sections 108 and 109, but these are narrow.

9.112 Our present view is that Part 10 should apply to all information matching programmes undertaken by public sector agencies. An agency should not be permitted to undertake information matching (within the meaning of Part 10) unless there is a specific statutory authority for it to do so and it undertakes information matching under and in accordance with that authority and Part 10.

9.113 Such an extension would also put beyond doubt that information matching involving public registers is subject to the usual controls, even though personal information in a public register is publicly available information and therefore exempted from principle 2.<sup>737</sup> The extension should also rule out reliance by agencies on the general law enforcement information regime in Part 11 of the Act (or whatever regime replaces it) as authority to undertake information matching.

9.114 We note that this extension of Part 10 would formalise the existing understanding that public sector agencies will not conduct information matching without specific statutory authority, and that new proposals should be subject to a rigorous process of justification and assessment before any such authority is granted.

Q108 We consider that all information matching undertaken by public sector agencies should require specific statutory authority, and be covered by the controls in Part 10 and Schedule 4. Do you agree?

<sup>736</sup> Paragraphs 9.32–9.35.

<sup>737</sup> With respect to public registers, see New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008).

### *Definition of “adverse action”*

- 9.115 The definition of “adverse action” in section 97 is of central importance to the operation of Part 10. Section 100 states that agencies can take “adverse action” against an individual on the basis of a discrepancy produced by an information matching programme in which the agency is involved. Sections 101 to 103 impose important procedural safeguards for individuals against whom agencies may take adverse action on the basis of a discrepancy.
- 9.116 The definition of adverse action states generally that it is any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual.<sup>738</sup> It then contains a non-exhaustive list of examples of decisions that fall within the term, such as a decision to cancel or suspend a social welfare benefit, to assess the amount of a tax or charge, or to investigate the possible commission of an offence.
- 9.117 While the list of examples is not exhaustive, the Privacy Commissioner, in *Necessary and Desirable*,<sup>739</sup> recommended that the definition be amended to include further examples of commonly occurring adverse actions. This would make the provision clearer and more helpful for agencies, and also as a consequence ensure that the procedural protections in Part 10 for individuals are complied with. It may well be thought that there are dangers in leaving it to an official to determine whether an action is adverse or not without clear guidance. The two kinds of decision identified by the Privacy Commissioner are a decision to impose a penalty, and a decision to recover a penalty or fine imposed earlier.
- 9.118 The examples listed in the definition of “adverse action” tend to reflect the kinds of action that were the focus of the first tranche of information matching authorities. As indicated above, the number and scope of these authorities have increased significantly since then. Except for the addition, in 2004, of a reference to certain decisions relating to immigration matters (such as a decision to deport), the list of examples has not otherwise been amended. We tend to support the Privacy Commissioner’s recommendations for additions to the list. However, we also consider that paragraphs (a) to (d) of the list, which relate to decisions with respect to monetary payments, could be condensed. Otherwise there is a danger that the list of decisions could become too long and unwieldy, and therefore less helpful.
- 9.119 We are also aware of a suggestion that the definition of “adverse action” should be amended to make it clear that information matching programmes that have a beneficial consequence for individuals (such as entitlement to a benefit not being claimed), or no adverse consequence (that is, a neutral consequence), are expressly excluded. This, it is said, would remove confusion among agencies as to whether or not they must comply with provisions such as the notice requirement in section 103, and when information provided for or derived from an information matching programme must be destroyed.

---

<sup>738</sup> Privacy Act 1993, s 97.

<sup>739</sup> *Necessary and Desirable* recommendation 117.

- 9.120 An example might be an information matching programme authorised by section 78A of the Births, Deaths, Marriages, and Relationships Registration Act 1995. Under this provision, the Registrar-General can obtain address information from the Ministry of Social Development in order to assist in locating and contacting the mothers of children whose births are unregistered so that their births may be registered. It is hard to see how registering an unregistered birth could be considered as an action that “may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual”.
- 9.121 It seems obvious that an action that has a beneficial or neutral consequence for someone is not an “adverse action”. We are not convinced that the suggestion to expressly exclude such actions from the definition has merit, and are more inclined to think that the clarification and simplification of sections 101 to 103 and Schedule 4 will serve the same purpose. Nevertheless, we would welcome any comments on the matter.

Q109 We propose that the list of examples of what constitutes “adverse action” against an individual should be extended to include a decision to impose a penalty, and a decision to recover a penalty or fine imposed earlier. Do you agree? Should any other changes be made to the list of examples?

Q110 We are currently of the view that the definition of adverse action should not be amended to clarify that information matching programmes that have a beneficial consequence for individuals or no adverse consequence are expressly excluded. Do you agree?

### *Computerised and manual matching*

- 9.122 In comparison with other jurisdictions, the New Zealand information matching provisions are unusual in applying to both computerised and manual matching. The US and Hong Kong legislation specifically apply only to computerised matching. The Australian Data-Matching Program (Assistance and Tax) Act 1990 does not expressly exclude manual matching, but the provisions relating to data matching and matching cycles clearly contemplate computer matching.
- 9.123 The Privacy Commissioner originally recommended in *Necessary and Desirable* that manual matching be excluded from Part 10 on the basis that the risks to privacy from data matching arise primarily from the automated or computerised nature of the exercise, and that no manual matching programmes had been brought within the ambit of the Part. This recommendation was subsequently withdrawn by the current Privacy Commissioner, because some computerised matching programmes may have a manual element. Removing manual matching entirely from Part 10 might therefore reduce the safeguards imposed by the Part.

9.124 We are inclined to the view that focusing Part 10 on computerised matching is appropriate and desirable, since that is where the primary risk to privacy lies. We therefore tend to the view that information matching programmes that consist of the manual comparison of personal information should be excluded from coverage. To the extent that some computerised matching programmes may have a manual element, it should be made clear that these are still covered. Again, we would welcome comments on this issue.

Q111 We propose that the controls on information matching programmes by public sector agencies should be focused on computerised/automated matching, and manual matching should no longer be covered (computerised information matching with a manual component would continue to be covered). Do you agree?

### *Information matching guidelines*

9.125 Under section 13(1)(f) of the Act, the Privacy Commissioner has the function of scrutinising legislative proposals involving the collection or disclosure of personal information by public sector agencies for the purposes of an information matching programme. In undertaking this scrutiny, the Privacy Commissioner is to have particular regard to the “information matching guidelines” set out in section 98.

9.126 The Privacy Commissioner has made three recommendations for amendment to section 98, designed to sharpen the analysis undertaken by agencies in preparing a proposal and so provide the Commissioner with better information on which to scrutinise the proposal.<sup>740</sup> The recommendations are as follows:

- Section 98(c) requires an assessment of whether or not an alternative means of achieving the objective of the proposed information matching programme would result in significant and quantifiable monetary savings, or in other comparable benefits to society. However, the provision does not require a consideration of whether or not the alternative means of achieving the objective would be more or less privacy-intrusive than the proposed programme. This is clearly an important consideration in deciding whether or not the alternative is preferable, and should be added.
- Section 98(e) requires an assessment of whether or not the proposed programme involves information matching on an excessive scale. In making this assessment, regard is to be had to the number of agencies to be involved in the programme and the amount of detail about an individual that will be matched. Additional considerations that should be added to section 98(e) are the amount of information disclosed as a result of a successful match, and the frequency of matches to be carried out under the programme.
- Agencies should be required to examine their proposed information matching programme against the requirements of Part 10, as well as the requirements of the privacy principles and the information matching rules.

<sup>740</sup> *Necessary and Desirable* 312–316, recommendations 122–124.

- 9.127 We agree with these recommendations.
- 9.128 It goes without saying that the ability of the Privacy Commissioner to properly assess a proposed information matching programme in accordance with section 98 depends in large part on the information provided to the Commissioner by the relevant agencies sponsoring the proposal. It has been suggested to us that a statutory requirement on the sponsoring agencies to supply the Commissioner with a written assessment of their proposal in the form of a “programme protocol” would highlight the need for agencies to undertake the necessary policy spadework when developing a proposal, and facilitate assessment of the proposal by the Commissioner.
- 9.129 As we understand it, the programme protocol would be a comprehensive document containing all relevant information about the proposed information matching programme. It would address each of the matters set out in section 98, as well as how the other control and reporting requirements in Part 10 and Schedule 4 would be complied with.
- 9.130 The programme protocol process is seen as a way of streamlining and bringing together a number of disparate processes so as to make the approval process for information matching programmes not only more efficient, but also more transparent. It is envisaged that the protocol would be made publicly available at the end of the process, and so facilitate compliance with the requirements of information matching rule 1 to promote public awareness of the programme.
- 9.131 We support the suggestion for a mandatory programme protocol procedure but we are open to alternative views on this point.

Q112 We propose that the information matching guidelines in section 98 should be amended to require a mandatory protocol procedure so that the Privacy Commissioner has better information on which to assess proposals for new information matching authorities. Do you agree?

### *Section 103: Notice of adverse action*

- 9.132 Section 103(1) currently provides that an agency must not take adverse action against an individual on the basis of a discrepancy produced by an information matching programme unless it has first provided notification, telling the individual that he or she has five working days from receipt of the notice to show why the action should not be taken, and waited for those five working days to expire. This is an important part of the post-match verification process, as it gives time for the individual to respond and point out if there has been an error.
- 9.133 The Privacy Commissioner recommended that the notice period be increased to 10 working days, on the basis that five working days is too short and a longer period would enhance the protection of individual rights that section 103 confers.<sup>741</sup> The equivalent period in Australian legislation is 28 days (20 working days).<sup>742</sup>

<sup>741</sup> *Necessary and Desirable* recommendation 128.

<sup>742</sup> Data-matching Program (Assistance and Tax) Act 1990 (Cth), s 11. In some circumstances, however, the Australian Act permits action to be taken without giving notice.

- 9.134 We also note that section 103 currently exempts certain information matching programmes from the requirement to wait until the expiry of the specified period before taking adverse action.<sup>743</sup> The requirement in section 103 has also been expressly overridden by other legislation.<sup>744</sup> It has been suggested that an alternative to specific statutory exemptions would be to confer a discretion on the Privacy Commissioner to shorten or waive the notice period in appropriate cases. We think that this would provide greater flexibility than the current method of blanket statutory exemptions and specific statutory overrides, and permit tailor-made arrangements that appropriately balance administrative considerations and the need to safeguard the interests of individuals.
- 9.135 We tentatively support both suggestions. We consider a 10-day notice period more appropriate. The provision of a discretion for the Privacy Commissioner to shorten or waive the notice period in section 103 should replace the need for statutory exemptions and overrides.

Q113 We propose that the period of notice that should be given by an agency before it takes adverse action against an individual on the basis of the results of an information matching programme should be increased from five working days to 10 working days. The Privacy Commissioner should also be empowered to shorten or waive the notice period in appropriate cases. Do you agree?

#### *Privacy Commissioner oversight, reporting, and review*

- 9.136 As set out above, the Privacy Commissioner plays a key role in overseeing the operation of information matching programmes, reporting to Parliament on their compliance with Part 10, and reviewing information matching authorities. For the most part, these processes work well. We have the following suggestions for enhancing them.
- 9.137 Currently, the Privacy Commissioner's annual report must include a detailed report on each information matching programme carried out during the relevant year. The Commissioner has recommended delinking the general annual report from the annual information matching reports, since finalisation of the Commissioner's annual report is unnecessarily delayed while waiting for the information matching reports to be received from agencies and analysed by the Commissioner. The Commissioner's report on the information matching programmes would be presented separately to Parliament.<sup>745</sup> We agree with this recommendation.

<sup>743</sup> See *Necessary and Desirable* recommendation 129. The Privacy Commissioner considered that the exemption in section 103(1A) was unnecessary and objectionable, and should be repealed.

<sup>744</sup> For example section 180C of the Corrections Act 2004 permits immediate suspension of benefits, allowances, and student loans as a result of a discrepancy produced by an information matching programme involving prisoners.

<sup>745</sup> *Necessary and Desirable* recommendation 131.

- 9.138 We have also considered the section 106 requirement on the Privacy Commissioner to review each information matching authority every five years. Two reviews covering six information matching programmes have been completed since 1994. Resourcing constraints have prevented both the current and the previous Privacy Commissioner from undertaking the regular reviews of information matching authorities required by section 106.
- 9.139 The review of authorising provisions for information matching is an important part of the overall system of oversight of information matching. Since these authorising provisions constitute an exception to the privacy principles, it is appropriate that each authority is regularly reviewed to establish whether or not it is still needed, whether or not the expected benefits from the programme are being realised and are sufficient to justify the inroads into privacy that the programme involves, and whether or not the actual operation of the programme over the review period provides sufficient confidence that the risks to privacy arising from the programme have been sufficiently well-managed to justify the continued existence of the programme.
- 9.140 In the absence of additional resourcing, an alternative to the review process might be considered. One option would be to “sunset” all information matching authorisations after a specified period (perhaps five years). The authority would lapse unless renewed by Parliament. The relevant agencies would have to justify the continuation of the authority to Parliament. A variation on this approach would be to provide for the life of information matching authorities to be extended by Order in Council, but provide that extensions could only be granted if the Privacy Commissioner had reviewed an Information Matching Privacy Impact Assessment and programme protocol for the programme and recommended that the extension be granted.
- 9.141 In addition, where the Privacy Commissioner does undertake a section 106 review, there is no requirement for the Government to respond to the Privacy Commissioner’s report. We suggest that there be a requirement on the Government to present a response to the House within six months of the presentation of the Commissioner’s report.

Q114 We propose that the Privacy Commissioner should be able to present a separate report to Parliament each year on his or her monitoring of information matching programmes, rather than include this in the Commissioner’s annual report. Do you agree?

Q115 We propose that, in the absence of increased resources to enable the Privacy Commissioner to undertake the required 5-yearly reviews of information matching authorities under section 106, each authority should be sunsetted so that it expires after five years unless (a) renewed by Parliament, or (b) extended by Order in Council made on the recommendation of the Privacy Commissioner. Do you agree? If so, which option do you prefer?

Q116 We propose that, if the Privacy Commissioner continues to undertake reviews of information matching authorities, there should be a requirement on the Government to respond to the Commissioner's report within six months of the presentation of the report. Do you agree?

#### *Exemptions for the Inland Revenue Department*

- 9.142 Section 101 and information matching rule 6 require agencies to either use information produced by an information matching programme to take adverse action against an individual, or destroy the information. The information cannot simply be held by the agency indefinitely. Adverse action must be commenced within 12 months from the date the information was produced, and the information must be destroyed when it is no longer needed for the purposes of taking adverse action against any individual. The source information disclosed for the purpose of the programme must also be destroyed if it does not reveal a discrepancy, or once it is no longer needed for the purposes of taking any adverse action.
- 9.143 The Inland Revenue Department (IRD) is currently exempt from all of these requirements with respect to every information matching programme. In *Necessary and Desirable*, the then Privacy Commissioner queried this blanket exemption.<sup>746</sup> He considered that any exemption for the IRD, if justified, should be conferred in the context of individual information matching authorities, and restricted to circumstances where the IRD is the end user of the information produced by a programme.
- 9.144 We think that a wider reconsideration of the current blanket exemption for the IRD is justified. It is hard to see why every agency other than the IRD is required to commence adverse action against an individual within 12 months from the date information is derived from an information matching programme. We share the Privacy Commissioner's concerns about the ability of the IRD to retain any information used in or derived from an information matching programme in which it is involved, regardless of whether it is the recipient or provider of the information.
- 9.145 It is our current view that the IRD's blanket exemptions should be repealed. Specific exemptions related to individual information matching authorities should be provided instead, if a good case can be made for them. Again, we welcome any comment on this point.

Q117 We propose that the Inland Revenue Department should no longer have a blanket exemption from the requirements to commence adverse action against an individual within 12 months, and to destroy personal information provided for or derived from an information matching programme once it is no longer needed. Specific exemptions for individual information matching authorities should be provided instead, if these can be justified. Do you agree?

<sup>746</sup> *Necessary and Desirable* para 10.6.4.

*Information matching rules*

- 9.146 The information matching rules in Schedule 4 are a mixture of general and detailed, technical requirements. They can be amended or replaced by Order in Council made in accordance with the recommendations of the Privacy Commissioner under section 107. However, some of the rules are so important or fundamental to the fair operation of information matching programmes that we think they ought to be stated in the body of the Act itself. This would mean that only Parliament could change them. We put the following rules in this category:
- *Rule 1:* This rule requires agencies involved in authorised information matching programmes to take all reasonable steps to ensure that individuals who will be affected by the programme are notified of it. Openness and transparency with respect to information matching programmes are important accountability mechanisms.
  - *Rule 7:* This rule prohibits agencies involved in an information matching programme from linking or merging the information used in the programme to create a new separate permanent register or databank of information about the individuals whose information has been subject to the programme. The rule is designed to prevent government agencies from using information matching to build up comprehensive profiles on individual citizens.
- 9.147 Those rules that are not of such a fundamental nature should remain in a schedule of the Act, and be subject to amendment or replacement by Order in Council. The technical nature of the rules justifies this degree of flexibility. Greater flexibility could also be introduced by authorising the Privacy Commissioner, in particular cases, to waive certain requirements in the rules, or grant exemptions from the requirements subject to conditions. This would reflect the fact that the rules must cover a wide variety of information matching programmes, and permit the Commissioner to tailor the information matching rules to cater for individual programmes.
- 9.148 We do not make further detailed recommendations about the information matching rules here. The Privacy Commissioner issued special reports in 2001 and 2003 recommending replacement of the information matching rules. These recommendations followed on from and built on the Commissioner's recommendations in *Necessary and Desirable*. The Commissioner described the objectives of the revision of the rules as follows: to express the existing rules more clearly; to provide new flexibility to recognise the diversity in authorised information matching programmes; to better integrate Part 10 and the rules; to use new concepts where appropriate to simplify meanings; and to enhance protections of individuals.

9.149 We would expect these recommendations to be taken into account in the preparation of any new legislation about information matching.

Q118 We propose that the current information matching rules requiring publicity and notice of information matching programmes, and prohibiting the creation of separate databanks, should be stated in the body of the Act itself. Do you agree? Are any other information matching rules so important that they should also be included in the Act rather than a schedule?

#### *Future-proofing Part 10*

9.150 Problems are sometimes encountered with respect to the application of Part 10 where agencies merge or their functions change.

9.151 One way of addressing this issue might be to empower the making of regulations amending the list of specified agencies in section 97 to ensure that the information matching controls in Part 10 continue to apply when agencies are reorganised.

Q119 Should the Act provide for the making of regulations amending the list of specified agencies in section 97 to ensure that the information matching controls in Part 10 continue to apply when agencies are reorganised?

#### *Other issues*

Q120 Do you have any other comments or suggestions about information matching?