

Part X

X

Information Matching

299

“The central element in any redistribution system is the identification of who should provide resources and who should receive assistance. Our present processes, involving repetition and poor coordination between agencies, are a result of the historical development of different aspects of redistribution at different times. In addition, they are related to the technological possibilities at the time when each part of the redistribution system was developed. We now have the opportunity to consider redistribution as an overall system and to contemplate addressing equity and efficiency issues as well as privacy concerns. It would be worrying to abandon individual privacy issues in the battle to avoid any benefit fraud. It would also be irresponsible to continue to preserve the existing system in the name of defending privacy. It would be possible to continue to provide the same degree of privacy protection as is enjoyed at the moment with a considerably increased degree of accuracy in the overall assessment processes.”

- Mark Prebble, *Information, Privacy and the Welfare State*, 1990

“Persons familiar with both matching programmes and the Privacy Act argue that they want to allow the use of new technology and at the same time protect individual rights. The question is how to achieve such laudable balance. There is probably little disagreement that computer matching should be carried out in a manner as to pose as little challenge as possible to the privacy interests of citizens, but the issue remains of how best to do this. If one agrees that the indiscriminate use of matching is in no-one’s best interests, who is going to set the appropriate limits?”

- David Flaherty, *Protecting Privacy in Surveillance Societies*, 1989

“Computer matching is a powerful dataveillance technique, capable of offering benefits in terms of the efficiency and effectiveness of Government business greater than its financial costs. However, it is also highly error-prone and privacy-invasive. Unless a suitable balance is found, and controls imposed which are perceived by the public to be appropriate and fair, its use will result in inappropriate decisions and harm to people’s lives. In a tightly controlled society, this is inequitable. In a looser, more democratic society, it risks a backlash by the public against the organisations which perform it, and perhaps also the technology which supports it.”

- Roger Clarke, *A Normative Regulatory Framework for Computer Matching*, 1995

10.1 INTRODUCTION

- 10.1.1 In preparation for this review I circulated, in February 1997, a questionnaire on Part X to government agencies which participate in information matching. The questionnaire was not intended to seek any “official departmental view” but instead to reflect the opinions or experiences of individual officials and to identify issues and possible options for reform. The respondents may not have expected to have their comments released in identifiable form and therefore I have not quoted directly from the responses or attributed them to particular individuals or departments.
- 10.1.2 In September 1997, a discussion paper was released. As the subject matter is relatively specialised it is perhaps unsurprising that only 14 submissions were received. It has become apparent to me that the information matching rules might benefit from a more thorough review than has been possible in this process. For that reason, some of my recommendations are expressed as matters for further consideration. That would provide a further opportunity for consultation with agencies involved in information matching on proposals for changes to the rules with the resulting changes implemented by Order in Council issued under section 107.
- 10.1.3 It is fair to say that Part X is relatively technical. It not infrequently gives rise to difficulties of interpretation even by those who work quite closely with it. Accordingly, a number of my recommendations are directed towards making the Part more plain, understandable and transparent. Among the suggestions that I have to achieve this is cutting the Part’s scope back to more realistically reflect the areas of concern. For example, I recommend that the Part no longer apply to any process of manual comparison and be restyled “data matching”. I also suggest that the specified agencies be listed alongside the relevant provision in the Third Schedule.
- 10.1.4 Before addressing the detail of Part X it is worth canvassing the reasons why the Act has a special part of it directed towards “information matching” or, more correctly, “authorised information matching programmes”. To understand this one needs to consider:
- what is information matching? and
 - why is it of concern?

What is information matching?

- 10.1.5 What the Act terms “information matching” is more usually known as “data matching” or “computer matching”.¹ There is no single settled meaning for the term “data matching” but the following definitions have been suggested from overseas:
- *data matching* is the computerised comparison of two or more sets of records; the objective is to seek out any records which relate to the same individual. Where there is such a “match” then the information from one set of records may be transferred to enhance the other set. Alternatively, the information on the matched individual may be extracted for decision and action and may form the basis of a further set of records. This new set may ultimately form a set of “profiles” of individuals drawn from a number of different sources;²
 - *computer matching* is the comparison of machine-readable records containing personal data relating to many people, in order to detect cases of interest;³

¹ Data matching is the term used in Canada, Australia and Hong Kong. The USA uses “computer matching”. New Zealand is the only jurisdiction to call the process “information matching”. Even in NZ the process is frequently referred to as “data matching” - with the main unit undertaking matching styled as the “National Data Matching Centre” of the NZ Income Support Service.

² Data Protection Registrar, *Eighth Report of the Data Protection Registrar*, June 1992, page 49.

- *data matching*: the large scale comparison of records or files of personal information, collected or held for different purposes, with a view to identifying matters of interest.⁴

These various formulations convey what the technical process is about.

- 10.1.6 Not all data matching programmes are alike. New Zealand, to date, has primarily authorised information matching programmes in two circumstances:
- to detect fraud and overpayments, particularly in the social security area;
 - to recover monies owed to the Crown by locating the whereabouts of debtors.
- 10.1.7 Although the two types just mentioned cover nearly all of the matches currently operated, there have been some other forays into data matching. For example, the process has been utilised in relation to verification of continuing eligibility for benefit programmes. One match, concerning eligibility for the Community Services Card is directed towards identifying persons who may not have claimed a benefit to which they are entitled. However, New Zealand has not utilised data matching in all its varieties as yet. Dr Clarke, a noted commentator on computer matching, has identified eight primary purposes for most matching of which New Zealand offers examples of only three or four. The eight primary purposes are:
- **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, etc;
 - **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**;
 - **updating of data** in one set of records based on data in another set.⁵
- 10.1.8 The practice of large scale data matching has only become possible with certain advances in computer technology and capacity. The first computer matching programme is sometimes claimed to be the one conducted in 1977 by the US Department of Health, Education and Welfare. That match compared the records of recipients of aid to families with dependant children with the payroll records of three million Federal employees.⁶ By 1982 it was estimated that US State and Federal agencies routinely carried out about 200 programmes which had apparently jumped to at least 500 by 1986. Experience suggests that the benefits of early matching, and its supposed successes, were wildly exaggerated whereas the problems at an operational level and for individuals affected were greater than had been anticipated.

Pros and cons of data matching

- 10.1.9 A great deal could be written about the perceived benefits and drawbacks of data matching. A number of people have attempted to do this. One report has

³ Roger Clarke, “A Normative Regulatory Framework for Computer Matching”, 13/4 *The John Marshall Journal of Computer & Information Law*, 587.

⁴ Australian Privacy Commissioner, *The Use of Data-matching in Commonwealth Administration Guidelines*, February 1998, clause 14.

⁵ Roger Clarke, “Computer Matching by Government Agencies: A Normative Regulatory Framework” (working paper August 1992), exhibit one. Dr Clarke also identifies a variety of circumstances in which data matching may contribute to additional purposes. For example, those with financial effects would include cancelling of incorrect payments, reduction of excessive payments, avoidance of future erroneous or excessive payments and deterrence of future fraudulent behaviour. Other purposes mentioned would include the maintenance of databases for social control purposes, construction of databases for research and statistical purposes, and improvement of programme policy, procedures and controls.

“Computer matching is like investigators entering a home without any warrant or prior suspicion, taking away some or all of the contents, looking at them, keeping what is of interest and returning the rest, all without the knowledge of the occupier.”

- AUSTRALIAN PRIVACY
COMMISSIONER

drawn together a list of claims made for data matching and the criticisms:

“The claims for data matching

Discussions in other countries have led to a number of benefits being claimed for the use of data matching. They include:

- detection and deterrence of fraud and other irregularities, for example, fraudulent or multiple claims, unreported income or assets, impersonation;
- verification of information supplied;
- verification of eligibility, for example for a benefit programme;
- identification of corruption or mismanagement, for example, conflict of interest; unusual payments; excessive withdrawals;
- construction of comprehensive databases for research purposes;
- identification of suspects through searching on the basis of the characteristics of potential offenders;
- improved efficiency, for example, in identifying and concentrating on genuine beneficiaries; or locating and rectifying discrepancies and errors;
- cost-effectiveness.

The criticisms of data matching

As benefits have been claimed, so there have been balancing criticisms of data matching. They include:

- lack of a general government or public oversight;
- cost/benefits are not thoroughly analysed so as to properly justify data matching programmes;
- poor quality and inaccurate information leads to mismatches and replication of errors;
- information is used out of context and may be untimely, insufficient, or unsuitable for the purpose of the match;
- information flowing from matching should be properly verified;
- machines should not be used as substitutes in qualitative decision-making for human discretion and judgment;
- the assembling of new files of profiles of individuals leads to the replication of inaccuracies and the drawing of what may be unjustifiable conclusions;
- individuals lack knowledge and control over the information about themselves;
- data matching constitutes a ‘fishing expedition’ without any pre-existing evidence or suspicion of wrongdoing;
- a presumption of innocence is turned into a presumption of guilt;
- individuals are not given any adequate opportunity to contest the results of a ‘match’;

“It is a technique which, unbridled, would present an Orwellian threat which even Orwell would not have imagined. The invasive indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.”

- CANADIAN PRIVACY COMMISSIONER

⁶ Details of this match, and information on the nature and origins of computer matching, can be found in Roger Clarke “Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism” 4/1 *Information Infrastructure and Policy* (1995) 32. Apparently this match identified 33,000 raw hits, later filtered to 7,100 resulting in 638 internally investigated cases, of which 55 resulted in prosecutions. Only 35 convictions, all for minor offences, were entered. Initially hailed as a success, the paltry measurable benefits only became apparent upon study and such origins have in part led to a subsequent focus on seeking to judge such costly schemes on a cost-benefit basis.

- profile searching in particular results in a mass or class investigation, conducted on a category of people rather than individual suspects;
- allowing different organisations to exchange personal data weakens the traditional concerns for confidentiality in each.⁷

Controls on data matching

10.1.10 The objectives of most regulatory controls on data matching are directed towards seeking to ensure or maximise the claimed benefits of data matching and to constrain or eliminate the perceived shortcomings. Most schemes have an authorisation process which judges the costs/benefits and permits only those programmes which appear likely to be worthwhile. The shortcomings of data matching are limited through various legal, operational and management controls together with independent supervision and redress for individuals who have been wrongly harmed by the process. Ongoing, or periodic, scrutiny is used to seek to ensure that the original claims were well-founded and the programme is operated in accordance with the rules laid down.

10.1.11 The United States was the first country to adopt a statutory scheme for the regulation of data matching. It was followed by Australia in 1990 and New Zealand in 1991. Meanwhile, the Canadians at Federal level had adopted an administrative scheme for the regulation of data matching and the Australians have since supplemented their statutory scheme with administrative controls for other programmes involving Federal agencies. In 1995 Hong Kong also regulated aspects of data matching by statute, although apparently in a less rigorous way than New Zealand, but with the novel feature that the controls apply equally to the public and private sectors.

Information matching not prohibited

10.1.12 Part X purports to regulate aspects of “information matching”. In fact, the Part does not regulate all information matching but only certain types of programmes, primarily those which will be used for the purpose of taking adverse action against individuals and which have been authorised by statute. As the scope of the Part is thereby quite limited I have recommended elsewhere it should be headed “*authorised information matching programmes*” rather than simply “information matching”.⁸ That small change may help to avoid misunderstanding by some people.

10.1.13 It is necessary to understand that Part X, and indeed the Privacy Act itself, does not contain a prohibition on data matching.⁹ This contrasts with the Hong Kong law which does prohibit data matching unless it has been appropriately authorised by the individual, the Commissioner specifically, or is of a class authorised by the Commissioner or by law.¹⁰ Generally the schemes in the USA, Canada and Australia only involve matches in which the Federal Government participates. Each scheme differs in the types of matches which are required to be brought within the controls or are exempted from them.

10.1.14 In 1991 the Privacy Commissioner Act first regulated information matching in New Zealand. Brought within its scope were all information matches known to be operated or intended soon to be operated. Government policy since that time has been to bring proposed new matches within the framework by enact-

⁷ Data Protection Registrar (UK), *Eighth Report of the Data Protection Registrar*, June 1992, pages 49-50.

⁸ See recommendation 2.

⁹ Section 108 does operate as a partial bar to information matching outside the controls of Part X where there already is an authorised information matching provision. Section 109 prevents the reliance upon the official information statutes to circumvent the controls on information matching in Part X.

¹⁰ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 30(1).

“What is wrong about ‘fishing expeditions’ is wrong about unrestrained computer matching: it changes the way a government looks at its citizens. Participating in a government programme is a status not a crime. To subject a whole class of citizens to search for possible violations is akin to a ‘general warrant’, a practice in England that permitted the Crown to search without specifically naming the target.”

- CANADIAN PRIVACY COMMISSIONER

ing an information matching provision which is added to the list in the Third Schedule. However, it is necessary to realise that only those matches which have been specifically authorised by a statutory “information matching provision” are covered by the controls in Part X. It is conceivable that matching programmes could exist or be created, not brought within Part X and yet still be in compliance with the law. For example, in addition to authorised information matching programmes covered by Part X, matches might exist as follows:

- a match authorised by a specific provision in legislation which has not been identified as an “authorised information matching provision”;¹¹
- a match carried out pursuant to general authority of an enactment which can be characterised as “authorising” or “requiring” the match which may override any inconsistent provision in an information privacy principle by virtue of section 7 of the Act;¹²
- a match undertaken by a department which is able to be carried out consistently with the information privacy principles or in reliance upon applicable exceptions to the principles (for example consistently with the purposes for which information is obtained or with individual authorisation);
- a match which is not in conformity with the principles but is otherwise authorised, for instance by an exemption granted by the Commissioner or pursuant to a code of practice.¹³

10.1.15 Generally speaking it would be difficult for a Government agency to carry out an information matching programme, and take adverse action against individuals, without seeking specific legislative authority. In the event that legislative authority is sought the Department will, by virtue of obligations in the *Cabinet Office Manual*, be obliged to address the question of compliance with the information matching controls. This in turn will normally require the relevant provision to be identified as an information matching provision in the Third Schedule.¹⁴

10.1.16 The principal compliance difficulties that departments would have in commencing a new information matching programme consistently with the information privacy principles include:

- the new programme will involve a collection of information from a source other than the individual concerned - therefore an applicable exception to information privacy principle 2 would need to be found;
- similarly, the programme will involve a disclosure of personal information for a new purpose and it may be difficult to find a relevant exception if authorisation of the individual is not possible or likely;
- at least one of the sets of information which is to be compared will be being disclosed to a new recipient, and being used for a new purpose, and it is unlikely that individuals will have been made aware of this in accordance with information privacy principle 3 - therefore a compliance issue arises as to the openness of the information handling practices of both departments if the match is to continue.

¹¹ There are several examples of these already. Through the process of consolidating various statutes some provisions which were listed in the 1991 Act had been inadvertently left out of the schedule to the 1993 Act for varying periods. Also, section 11A of the Social Security Act is not listed as an information matching provision but nonetheless provides that it is, for a number of purposes, to be treated as if it is.

¹² Pursuant to government policy these and those in the next category should be created as information matching provisions and subjected to Part X.

¹³ A series of one-off exemptions were granted by the Privacy Commissioner pursuant to section 54 for a series of comparisons of information similar to information matching in 1995/96. See report of the Privacy Commissioner for the year ended 30 June 1997, page 25.

¹⁴ See *Cabinet Office Manual*, August 1996, chapter 5, paragraph 5.26, 5.29 and 5.58 and Appendix 6 (Standard format for legislation submissions).

10.1.17 Notwithstanding the practice and policy of bringing new matches within the Third Schedule there have been cases where it has been inappropriate to do so. The most common such circumstance is where a match is to be undertaken for statistical or research purposes and not to enable adverse action to be taken against an identifiable individual. Where departments are contemplating seeking authority for a new matching programme I have encouraged them to undertake a pilot statistical match so as to generate empirical data by which the likely usefulness, and the cost benefit, of a prospective match may be projected and judged. Safeguards are taken by the departments to ensure that the data is destroyed or de-identified once the necessary statistics have been extracted. I have seen the “statistical and research purposes” exceptions to principles 2, 3 and 11 as providing sufficient authority for such pilot matches to be undertaken.

10.1.18 Another case involved the transformation of an existing process of manual verification of jury lists into an automated process. For many years information extracted from the electoral roll had been sent to court registrars from which a jury list is drawn. Preliminary steps are taken to omit names from the list of persons who are ineligible to serve. The practice has been for potential jurors’ names to be checked against the criminal history listing on the Wanganui Computer. This had been done by a Court official checking each name individually through the Court terminal to the computer. This would not have been characterised as an “information matching programme” as defined in section 97. However, to modernise court administration it was proposed to automate the process. The list of potential jurors would be matched against the Wanganui Computer list of relevant convictions. It is difficult (although not impossible) to characterise the omission of a name from the list of potential jurors as “adverse action” as it is normally understood. Having considered various aspects of the process it was not considered appropriate to bring it within Part X.

10.1.19 One confusing aspect of Part X is therefore the position of the matching programmes which are *not* authorised. This will continue to be a source of confusion for those unfamiliar with Part X. It is difficult to address the matter without fundamentally changing the approach of Part X which I have not attempted in this review.

Legitimising data matching

10.1.20 It is as well to reflect at this point that the Privacy Act 1993 fulfils a function of *legitimising* information matching. Whether this is predominantly good or predominantly bad for privacy is a moot point. 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 brings the activity within a satisfactory structure which places a set of controls, subject to independent oversight, directed to:

- *authorisation* - ensuring that only matches which appear to be well justified in the public interest go ahead;
- *operation* - ensuring that matches are operated consistently with fair information practices and, given the nature of the technique, that individuals are not presumed guilty until they prove their innocence;
- *evaluation* - that matches are subject to periodic review and discontinued unless they show continuing benefits and the ability to be operated consistently with fair information practices.

It may also be that, on occasion, information matching may be less privacy invasive than alternative methods of detection of possible fraud.

“A traditional investigation is generally triggered by some evidence that a person is possibly engaged in wrongdoing. A computer match is not bound by this limitation. It is directed not at an individual, but at an entire category of persons. It is random in nature as it is not initiated because any person is suspected of misconduct, but because a category is of interest to the Government. What makes computer matching fundamentally different from a traditional investigation is therefore that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin.”

- ONTARIO INFORMATION AND PRIVACY COMMISSIONER

SECTION BY SECTION DISCUSSION

10.2 SECTION 97 - Interpretation

Further definitions

- 10.2.1 Section 97 sets out definitions used throughout Part X. The general definitions in section 2 also apply. I am aware of occasions where staff in agencies undertaking information matching have forgotten to look to that earlier section for relevant definitions such as that of “working day”.
- 10.2.2 Only nine terms are given specific definitions for Part X. There has been a tendency amongst agencies working in this area to coin a variety of other terms to describe the various information matching concepts. Indeed, in a paper for the Second Privacy Issues Forum in Wellington in 1995, the National Data Match Co-ordinator for the Department of Social Welfare, offered working definitions for twelve terms neither used or defined in the Privacy Act:¹⁵
- challenge;
 - invalid match;
 - legitimate match;
 - match-run;
 - match-run date;
 - matching agency;
 - mismatch;
 - no further action;
 - partial positive match;
 - positive match;
 - record count;
 - source agency.
- 10.2.3 I suggest below that “source agency” and “matching agency” should be defined.¹⁶ I also suggest that it might be possible to use the information matching rules to address definitional problems given the special amendment procedure in section 107.¹⁷ However, I see no need for any large number of further definitions.

Adverse action

- 10.2.4 The definition of “adverse action” has caused difficulty for staff in some agencies involved in information matching. The concept of adverse action is primarily applied in sections 101, concerning the use of the results of an information matching programme, and section 103, providing for notice of proposed adverse action to be sent to individuals.
- 10.2.5 The Privacy of Information Bill had no definition of “adverse action”. Instead the concept appeared in a composite provision being the equivalent to sections 100 and 101. That had as its origin sections 10 and 11 of the Data-matching Program (Assistance and Tax) Act 1990 (Commonwealth of Australia). The Australian Act is therefore the origin of the concept of “adverse action” although the term is not actually defined there. The Hong Kong privacy law has adopted the first part of the New Zealand definition but has additionally referred to “legitimate expectations” and omitted the specific examples in paragraphs (a) to (f) of the New Zealand definition.¹⁸
- 10.2.6 The reason that some people have had difficulty with the definition is that they

¹⁵ Dallas Elvy “Information Matching”, Privacy Issues Forum, 29 June 1995.

¹⁶ See recommendation 121.

¹⁷ See recommendation 137.

¹⁸ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 2, defines “adverse action” in relation to an individual to mean “any action that may adversely affect the individual’s rights, benefits, privileges, obligations or interests (including legitimate expectations).”

have failed to notice that it encompasses actions that *may* adversely affect the rights etc of specific individuals. That, of itself, seems to indicate that the concept encompasses actions taken or anticipated quite early in the processes following the carrying out of an information match. It is an action which has the potential to affect the rights of a specific individual and not simply the later action which does directly affect that individual. This is made plainer by the second part of the definition which makes it clear that such action includes “any decision” to do certain things in relation to the individual. Difficulties that have arisen with the interpretation of the term are not because the definition itself is particularly unclear but because departments have found it inconvenient to accept the provision’s plain words. The term is defined as it is in order that the controls in sections 100, 101 and 103 should be applied at a very early point in the process and not, as some departments would wish, after preliminary steps which may affect individuals’ interests have already been taken.

- 10.2.7 Responses to the questionnaire noted that paragraph (a) to (f) did not cover all of the commonly occurring circumstances of adverse action. From a definitional point of view, this need not matter particularly so long as the relevant action can be said to “adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual” (that is, within the first part of the definition). However, from a practical and operational point of view it would be helpful for all of the common examples to be listed so as to make the position more plain. I have two suggestions.
- 10.2.8 The first suggestion is to include the phrase “to impose a penalty”. This is numerically, and financially, important in the context of the DSW programmes.
- 10.2.9 The second relates to the recovery of a penalty imposed by a department and of a fine. In this context the word “decision” may confuse the issue for some when the position is that someone has already been covered by a decision to recover money, but the department could not find the miscreant, and now as a result of address matching is able to take further steps to recover the fine. The concept of “adverse action” is intended to apply in such circumstances and I take the view that it does even as presently drafted. However, it may be helpful to agencies operating address matches used to trace and enforce Court ordered obligations for the second part of the decision to be made more explicit.



RECOMMENDATION 117

The definition of “adverse action” in section 97 should be supplemented by a paragraph relating to decisions to impose a penalty and to recover a penalty earlier imposed.

Authorised information matching information

- 10.2.10 This definition seems relatively plain and has not given particular difficulty in interpretation. Some of the information matching provisions are more particular than others in the authority they give for the disclosure of information. In my view, information matching provisions should precisely list the information which may be disclosed.

Authorised information matching programme

- 10.2.11 The definition of “authorised information matching programme” surprisingly does not simply constitute an “information matching programme” (as defined) which has been authorised. In fact, the definition repeats several elements of the definition of “information matching programme” (such as the comparison of information with the purpose of producing or verifying information) but omits other elements (such as the requirement that the information may be used for the purpose of taking adverse action against an identifiable individual).
- 10.2.12 It is not immediately apparent why the differences in definition have been

“We view data matching as a procedure which poses a number of data protection dangers and believe that safeguards are warranted where it exposes data subjects to adverse decisions. Not all data matching does so, but when it does controls are in our view desirable.”

- THE LAW REFORM COMMISSION OF HONG KONG, *REPORT ON THE REFORM OF THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA*, 1994

adopted. Perhaps it was anticipated that authorised programmes might encompass a wide range of matching including that which did not have as its purpose the taking of an adverse action against identifiable individuals. If that was the intention, the approach has since been somewhat haphazard. The Community Services Card Match is the only authorised programme which is not used for taking an adverse action against individuals. Perhaps the reason for adopting the perplexing definition is found within section 108. That is the only provision which utilises within it both “authorised information matching programme” and “information matching programme”. There may be scope for simplifying the definition. If that is to be done, care would need to be taken to ensure that section 108, and any other affected provision, is not inadvertently changed in substance.

Discrepancy

10.2.13 The definition is derived from the definition of “discrepancy” in the Australian legislative scheme.¹⁹ I do not consider that it requires amendment.

Information matching programme

10.2.14 The definition of “information matching programme” has several elements. Features to note include:

- an information matching programme involves the comparison of any document that contains personal information about ten or more individuals with one or more similar documents;
- the comparison may be made manually or by means of any electronic or other device;
- the comparison must be for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual.

10.2.15 This definition potentially encompasses a far broader range of programmes than most overseas schemes or definitions.²⁰ No comparable scheme overseas provides for oversight of, or safeguards in relation to, manual matching. For example, the definition of “matching procedure” in the Hong Kong law is quite similar to our own definition of information matching programme but expressly excludes comparison by “manual means.”²¹

10.2.16 The concern to which the information matching controls are directed relate to what is commonly known as *computer* matching or *data* matching. Nonetheless, as a definitional matter it was decided, consistent with the rest of the Act, to avoid distinctions based upon:

- whether the processing of information is by automated or manual means; or
- whether the information is stored in electronic or other media.

10.2.17 The special data matching controls in New Zealand, USA, Australia, Canada, Hong Kong and other countries have arisen from concerns about automatic processing of information and, particularly, the use of computers for covert surveillance. Dr Roger Clarke, a commentator on data matching, describes the processes of concern as “dataveillance”. He distinguishes two types: personal dataveillance, in which an identified person is monitored, generally for a specific reason; and mass dataveillance, in which groups of people are monitored, generally to identify individuals of interest.²² The controls of the type found in our Act and similar legislation are directed towards mass dataveillance. It is

¹⁹ Now found in Data-matching Program (Assistance and Tax) Guidelines, clause 2.2.

²⁰ However, note that while “information matching programme” is a broad definition, Part X itself tends only to cover *authorised* information matching programmes.

²¹ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 2(1).

²² See Roger Clarke, “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law* (1995) 585.

hardly possible to imagine mass dataveillance without the use of automated processes of comparison. Even if mass dataveillance might be theoretically possible on a manual basis, it would be uneconomic.

- 10.2.18 A further concern (and another distinguishing manual from automated matching) is the involvement of human beings. One of the fears of data matching is that machines will be programmed in such a way that decisions affecting individuals are made without any real person considering the facts of an individual case. The EU Directive on Data Protection articulates such concerns in article 15 by providing special controls on automated individual decision-making.
- 10.2.19 The special controls in Part X, which operate as a specific regime within a more general statute, may be more effective and better understood where the key concepts correspond to the risks designed to be addressed and the reality on the ground. The present reality is that there are no “manual” matches authorised. I see little prospect of any being brought within Part X. It might be desirable to limit Part X to the area of prime concern and therefore to exclude manual comparison from its coverage.²³
- 10.2.20 Exclusion of manual matching from the scope of Part X could be achieved by providing an exception to the definition of “information matching programme” and “authorised information matching programme”. This is the approach taken in Hong Kong. Alternatively, the definition could be recast so that the notion of “computerised” or “automated” comparison is incorporated as an element. This is the approach taken in the USA.²⁴ The result appears to be the same either way.



RECOMMENDATION 118

Consideration should be given to amending the definitions of “authorised information matching programme” and “information matching programme” in section 97 so as to exclude manual comparison from their scope.

- 10.2.21 If manual matching is excluded, the process should be given an explicitly narrower title such as “computer matching” or “data matching” which suggests the involvement of automated processes. I favour data matching as this appears to be the term which has the widest currency internationally and is frequently used domestically. It is possible to label the process as “data matching” without needing to define, or use, the term “data” anywhere in the Part. The process can be styled as “data matching” while still referring to the comparison of “information” so as to remain consistent with the rest of the Act.



RECOMMENDATION 119

Consideration should be given to replacing references in Part X and elsewhere to “information matching” by “data matching”.

Information matching provision

- 10.2.22 I am unaware of this definition causing any difficulties in interpretation.
- 10.2.23 There were ten sections listed as information matching provisions when the Privacy Commissioner Act 1991 was first enacted.²⁵ Most of the Schedule from the 1991 Act was carried over into the Act and subsequently three of the original provisions, never used, were omitted with the enactment of the Births, Deaths and Marriages Registration Act 1995. With the addition of new infor-

²³ I use the shorthand expression “manual matching” but it is the process of *comparison* where the computer comes into its own. A programme might well have other manual components in the obtaining, disclosure or the use of information. For this reason the spelling of “programme” should remain rather than the computer-oriented “program”.

²⁴ Privacy Act 1974 (USA), 5 USC §552a (8).

²⁵ Privacy Commissioner Act 1991, Third Schedule.

mation matching provisions there are now thirteen sections listed in the Third Schedule as information matching provisions. Bills before Parliament are poised to add several more.

Information matching rules

- 10.2.24 The phrase “information matching rules” is defined to mean the rules for the time being set out in the Fourth Schedule to the Act. Proposals for amending the rules are made with the material discussing sections 107 and the Fourth Schedule.²⁶

Monetary payment

- 10.2.25 I am not aware of this definition giving rise to any interpretational difficulties. Indeed, it has been suggested to me that the definition is quite unnecessary.

Specified Agency

- 10.2.26 “Specified agency” is defined simply to mean any of the agencies listed in the provision. The list has been amended from time to time with the addition of certain agencies, substitution of new names for restructured departments, and in one case the removal of an agency as the result of the repeal of particular information matching provisions.

- 10.2.27 The present definition of “specified agency” gives the somewhat misleading impression that Part X legitimises an arrangement whereby a group of eight agencies may share personal information amongst themselves. Indeed, this is precisely what an Opposition member of Parliament alleged on the Third Reading of the Privacy Commissioner Bill in which he stated:

“So the bill establishes what really amounts to a club - I mean in the insurance club sense of the word. A group of agencies - eight in number - now has a mandate to match information and to share it.”²⁷

- 10.2.28 In fact, there is not a multiple sharing arrangement amongst all eight agencies but rather a series of bilateral arrangements between particular specified agencies pursuant to particular information matching provisions. This is not particularly plain from reading Part X or the Third Schedule but becomes clearer once a study is made of the various information matching provisions. In fact, it is only possible to know whether a specified agency participates in one or more information matching programmes and, if so, which and in what capacity, by studying a raft of provisions in other statutes. Transparency would be enhanced by redefining “specified agency” in the following manner:

Specified agency means any agency listed in the third column of the Third Schedule as a specified agency in respect of an information matching programme authorised pursuant to an information matching provision specified in the first column of that Schedule.

- 10.2.29 One will then be able to see by a simple check of the Third Schedule:
- which programmes an agency is involved in; and
 - which agencies are involved in a particular programme.



RECOMMENDATION 120

The definition of “specified agency” in section 97 should be amended so that the agencies are listed in the Third Schedule alongside the information matching provisions to which they relate.

²⁶ See paragraphs 10.12 and 13.5.

²⁷ Rt Hon. David Lange, speaking on the third reading of the Privacy Commissioner Bill, 10 December 1991.

- 10.2.30 All the agencies participating in an information matching programme are referred to as “specified agencies” regardless of the capacity in which they participate. This contrasts with the schemes in North America and Australia which label agencies by their function in a programme. By categorising the agencies it has been possible in those other schemes to separately identify some of the requirements of the regulatory scheme to apply to certain classes of agencies and not others.
- 10.2.31 Some schemes use a term to identify the totality of participants in a scheme. This corresponds with our present definition of “specified agency”. In the Australian statutory scheme this is simply referred to as an “agency”.²⁸ In a scheme devised by Dr Clarke the term used is “a participating organisation”.²⁹ The second categorisation used by most schemes is to identify the agency which discloses the records for the use in a matching programme. This is referred to as a “source agency” in the schemes in the USA and Australia (both under the statutory scheme and pursuant to the Privacy Commissioner’s guidelines) and as “matching source” in Canada. In each case, a definition is provided to the effect that a source agency is one which discloses information to a matching agency for use in a data matching programme. Typically the third category is “matching agency” which is the agency on whose computer facilities the matching is conducted. The scheme in the USA instead refers to a “recipient agency” being the agency which receives the information from the source agency for use in a matching programme.
- 10.2.32 Logically, there should be a further category of agency which is authorised to *use* the resultant “hits”. In New Zealand, this has always been either the source or the matching agency,³⁰ although it does not follow that this will always be the case. “User agency” seems an obvious choice and this is adopted in the Australian Privacy Commissioner’s guidelines.
- 10.2.33 Definitions of the new terms should be supplemented by identification of each agency as an authorised “source agency”, “matching agency” and/or a “user agency”. The Third Schedule should list, against the information matching provisions to which they relate, each of the specified agencies and the capacity in which they participate. Some agencies will participate in a match in more than one capacity, as a user agency and matching agency or as a user agency and source agency.
- 10.2.34 Defining these concepts, and identifying the agencies in their respective capacities in the schedule, will enable the statutory scheme to be more transparent. However, the full benefit will only be realised when the opportunity is taken to rewrite some of the material in Part X and the Fourth Schedule utilising the newly defined terms. That will enable some provisions to be set out in a clearer or more precise fashion. In others it may be possible to allocate certain statutory obligations to some classes of agencies but not others. I recommend elsewhere that a more detailed review of the information matching rules be undertaken at a later date which I think will offer a good opportunity to bring the new terms into use in a clear and understandable manner. I expect that the terms will also be useful in information matching agreements entered into under section 99.

²⁸ Data-matching Program (Assistance and Tax) Act 1990, section 2(1).

²⁹ Roger Clarke, “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law*, 619.

³⁰ Indeed, locally a somewhat confusing terminology has grown up, at variance with the international approach, according to the agency which is to be the primary user of the information the title “matching agency” regardless of whether it has actually carried out the comparison of records.

**RECOMMENDATION 121**

Consideration should be given to:

- (a) including in section 97, in addition to the definition of “specified agency” (which could be renamed “participating agency”), definitions of “source agency”, “matching agency” and “user agency”; and
- (b) utilising these newly defined terms in Part X and the Fourth Schedule as appropriate.

10.3 SECTION 98 - Information matching guidelines

10.3.1 Section 98 sets out the six information matching guidelines. Section 13(1)(f) requires the Privacy Commissioner to have particular regard to the guidelines when examining proposed legislation which would provide for information matching. The Commissioner’s function under section 13(1)(f), and the process adopted for undertaking that examination, are outlined at paragraphs 3.3.36 - 3.3.42.

10.3.2 When introduced in the Privacy of Information Bill, the information matching guidelines were to have been the grounds upon which the Privacy Commissioner could grant, upon application by a department, approval for an information matching programme. This was changed by the select committee so that the decision as to whether an information matching programme proceeds is one for Parliament, not the Commissioner. However, the information matching guidelines have been retained to guide the Commissioner when examining a proposed programme and reporting to the Minister of Justice.

10.3.3 The information matching guidelines have not been taken directly from any precedent in a New Zealand or overseas law. However, the basic approach, and elements of the guidelines, can be found in similar sets of requirements for data matching proposals in other jurisdictions. For example, many of the elements are similar to those found in the Australian Privacy Commissioner’s *Guidelines for the Use of Data Matching in Commonwealth Administration*,³¹ the Canadian Treasury Board Manual,³² and the Computer Matching and Privacy Protection Act 1988 (USA).³³

10.3.4 The schemes providing for control of data matching in the USA, Canada, Australia and New Zealand each emphasise the need to evaluate any proposed programme on a cost-benefit basis before allowing them to proceed. The reasons for this approach have been outlined in a variety of governmental reports.³⁴ There has also been scholarly analysis of the reasons for undertaking cost-benefit analysis.³⁵ Briefly stated the reasoning goes something like this:

- data matching is an activity which can severely intrude on privacy;
- data matching has the potential to uncover fraud, and recover monies owed to the government, and therefore in some cases the effect on privacy may be outweighed;
- experience has shown that the claimed benefits of data matching have been wildly exaggerated while the costs, financial and otherwise, have been underestimated;
- therefore, cost-benefit analysis is needed to ensure that privacy is only al-

³¹ The current version is dated February 1998. See clause 32 (“Proceeding with a programme”).

³² Treasury Board of Canada, *Treasury Board Manual*, Chapter 2-5 (Data matching), Preliminary assessment, pages 1-2 (current version 1 December 1993).

³³ To be read together with guidelines issued by the Office of Management and Budget.

³⁴ See for example, United States General Accounting Office, *Computer Matching: Assessing its Costs and Benefits*, September 1986.

³⁵ See, for example, R Clarke “Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism” 4/1 *Information Infrastructure and Policy* (1995) 29 and “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law* (1995) 585.

“After four full years of operation the cumulative savings from the programme are \$210 million across all agencies. It is interesting to note that to date the total net savings from all agencies remain less than the DSS anticipated it would save in one year.”

- KEVIN O’CONNOR, PRIVACY

COMMISSIONER OF AUSTRALIA,

EIGHTH ANNUAL REPORT ON THE

OPERATION OF THE PRIVACY ACT,

1996



lowed to be overridden in cases where it can confidently be shown that a data match will indeed bring quantifiable and commensurate public benefits.

- 10.3.5 The monetary savings are only one part of the equation. There is a privacy concern to ensure that the matches justified for their net financial benefit can be and are undertaken in accordance with fair information practices. Considerable experience has been gathered in the USA, Canada, Australia and now New Zealand, in evaluating and operating information matching programmes so that the worst excesses of data matching experienced in the past are not repeated. Accordingly, the initial assessment not only looks to net financial benefit but also to assurances that any programme will be operated in conformity with a set of information matching rules and controls.
- 10.3.6 Although there is not an absolute demarcation, generally speaking the first four of the six information matching guidelines are directed towards financial considerations with the last two guidelines addressing what might be termed “data protection” or “fair information practice” concerns.
- 10.3.7 It is unnecessary in this report to go into detail about the information matching guidelines since, with the exception of several relatively minor matters raised below, the guidelines have worked satisfactorily in operation and are not in need of amendment. I have offered detailed comment in relation to each of the guidelines in seven information matching programmes, or amendments to programmes, that I have examined and reported upon pursuant to section 13(1)(f). Copies of the reports and extracted comments on each of the guidelines have recently been published in a compilation.³⁶
- 10.3.8 I have four suggestions for change to the information matching guidelines. The first proposes a change to paragraph (c). The next two involve minor changes to paragraph (e) which will amplify upon the guideline but not change it substantively. The final suggestion is to alter paragraph (f) to expand its scope beyond compliance with the information matching rules to encompass compliance with Part X itself.

Paragraph (c)

- 10.3.9 Paragraph (c) requires consideration to be given to whether or not the use of an alternative means for achieving the match’s objective would give results of the type mentioned in paragraph (b), that is that it will achieve significant and quantifiable monetary savings or other comparable benefits to society. It would be worthwhile amending this paragraph so that consideration is also given to whether the alternative means of achieving the objectives are more, or less, privacy intrusive. The existing paragraph appears to assume that any other means of achieving the objective will give a better result for privacy. However, while that will often be true, it is not invariably the case.



RECOMMENDATION 122

Section 98(c) should be amended so that alternative means of achieving the objective of a proposed matching programme are examined with a view to considering whether they would be more, or less, privacy intrusive.

Paragraph (e)

- 10.3.10 Guideline (e) requires me to look at whether the scale of the matching programme is “excessive”. The guideline further requires me to have regard to the number of agencies that will be involved in the programme and the amount of detail that will be matched. I have not read guideline (e) as limiting me solely

³⁶ See Office of the Privacy Commissioner, Examination of Proposed Information Matching Programmes, March 1998.

to having regard to the number of agencies and the amount of detail matched if there is some other factor involved in the information matching programme which suggests that its scale is excessive.

- 10.3.11 It occurs to me that it would be relevant to consider, in seeking to gauge whether a match is “excessive”, the amount of information disclosed from one agency to another following a successful hit or match. I have had to consider this precise issue in the context of an amendment affecting the information matching programme between the Department for Courts and DSW³⁷ and in a similar proposal for a match between the Department for Courts and the Inland Revenue Department.³⁸ The amendment affecting the Courts/DSW match would, for the first time, have permitted DSW to disclose client telephone numbers to Courts. Prior to this amendment the information matching provision had merely authorised the disclosure of address details. The issue for me was whether the disclosure of additional information, in this case telephone numbers, might make the match “excessive”. In an examination of the subsequent Courts/IRD match I observed:

“The guideline directs me to consider whether the programme involves information matching ‘on a scale that is excessive’ having regard to ‘the amount of detail about an individual that will be *matched* under the programme’. The word ‘matched’ is not defined and I think it makes most sense in this context for the term to mean something like ‘used or disclosed’ rather than simply ‘compared’. For instance, telephone numbers will not be compared in this match but, where there is a hit, IRD will disclose to Courts the taxpayer’s telephone number ... The authorised disclosure of information as a result of the match is an integral part of a ‘matching programme’. It would be quite inadequate for me to judge whether a programme is ‘excessive’ solely on the basis of the details being compared, if as a result of that match, huge quantities of data on individuals are to be disclosed to the matching department in relation to successful hits”.³⁹

- 10.3.12 It would be desirable to refer specifically to the amount of information disclosed as a result of the match. It seems to me that this is consistent with a full examination of whether a programme is “excessive” in scale. I believe it would be desirable for the matter to be considered expressly in this context.
- 10.3.13 Another aspect relevant to whether a match is “excessive” is the frequency of matches. One of the existing matches is operated once each year. At the other end of the scale there is an on-line match which occurs a number of times each day. If frequency is explicitly mentioned in the guideline (e) then departments in their Information Matching Privacy Impact Assessments⁴⁰ will expressly address the question and make their intentions plain. It may be that the departments conclude that an annual or semi-annual match is sufficient as against, say, a monthly or fortnightly match. Where there is a good case for a frequent match this will not, of itself, render it “excessive”. Rather, it is a matter of the frequency being proportionate to the character and objectives of the match.

³⁷ See Report by the Privacy Commissioner to the Minister of Justice on an Examination of a proposal to amend section 126A Social Security Act 1964, August 1997.

³⁸ See Report by the Privacy Commissioner to the Minister of Justice on an Examination of a provision in the Summary Proceedings Amendment Bill (No 3) inserting an information matching provision into the Tax Administration Act 1994, March 1998.

³⁹ *Ibid.*, paragraph 3.5.3.

⁴⁰ The IMPIA process is discussed at paragraphs 3.3.40 - 3.3.42.

**RECOMMENDATION 123**

Section 98(e) should be amended so that in considering whether a programme involves information matching on a scale that is excessive, regard is also had to:

(iii) the amount of detail about an individual that will be disclosed as a result of the programme; and

(iv) the frequency of matching.

Paragraph (f)

- 10.3.14 Guidelines (d) and (f) provide for a proposed programme to be judged against the requirements of the information privacy principles and the information matching rules. However, the controls placed on authorised information matching programs are not simply found in the principles or rules but also in Part X of the Act itself. It would make sense for a proposed matching programme to be examined in advance for its prospective compliance with Part X.
- 10.3.15 I have emphasised in my dealings with departments the need to carefully work through their proposed operating procedures to ensure that there will be no difficulty in compliance with Part X. However, my experience has been that departments have nonetheless got themselves into compliance difficulties which has, in turn, made my job of monitoring compliance with the information matching controls quite difficult.
- 10.3.16 The main example of this, referred to often in my annual reports, has been the inability of the Department of Social Welfare to report to me satisfactorily on the operation of programmes in the manner or detail that it contemplated by section 104. Another example is the operation of the NZ Employment Service-NZ Income Support Service match in which it was discovered after the information matching provision had already been enacted that the departments could not comply with the periods allowed in Part X for the service of notices.⁴¹ A final illustration, concerns one department which continues to debate the need for the notices contemplated by Part X being given in the particular match because it asserts that other safeguards ought to suffice (a point, incidentally, that I do not accept).
- 10.3.17 However, whatever the merits of departmental cases for reporting, serving notices, or giving notices, the point is that any department should make the issue plain, and plead its claimed “special case”, before receiving the authorisation to carry out the match. It is quite unacceptable and inefficient for the match to be authorised and be subject to Part X and only *then* for a department to start raising issues. Departments seeking authorisation for an information matching programme under Part X are, quite sensibly, assumed to know that they will be subject to Part X and it is understood that they will, of course, comply. For the most part that is a sound assumption. However, experience suggests that the matter ought to be made explicit so that programmes will be assessed, in advance, to ensure that they will comply not only with the information matching rules but also Part X.
- 10.3.18 Sometimes departments will seek a dispensation or authorisation within their information matching provision. This should not routinely happen since the scheme of Part X, and the information matching rules, provide a regime for the systematic control of information matching to appropriately protect privacy and meet the needs of other public interests. Nonetheless, there may well be some special circumstances needing, in essence, an exemption from one or more of the information matching rules or perhaps aspects of Part X. If an information matching provision so provides it will likely override a contrary provision in Part X (through the normal rules of statutory interpretation whereby a spe-

⁴¹ See Report of the Privacy Commissioner to the Minister of Justice on the Social Security Amendment Bill, April 1997.

cific provision prevails over a general provision, and a later statute prevails over an earlier one). However, by incorporating reference in information matching guideline (f) to compliance with Part X this can be more clearly taken into account in the examination and authorisation processes.



RECOMMENDATION 124

Section 98(f) should be amended so that the information matching guideline refers not only to the information matching rules but also to Part X of the Act.

10.4 SECTION 99 - Information matching agreements

10.4.1 A written agreement is necessary between the relevant agencies before personal information held by one specified agency may be disclosed, pursuant to an information matching provision, to another for the purposes of an authorised information matching programme. The agreement must incorporate provisions that reflect the information matching rules, or provisions that are no less strict than those rules, and the agencies concerned must comply with those provisions. A copy of the agreement, and any subsequent amendments, must be forwarded to the Privacy Commissioner without delay.

Upside

10.4.2 A clear written agreement between the parties to an information matching programme is also a feature of North American schemes for controlling data matching.⁴² I expect that in those jurisdictions where agreements are not formally required the relevant agencies would, in any case, execute such agreements. An agreement is valuable for a number of reasons and it helps ensure that all parties are aware of their obligations.

10.4.3 Two suggestions for amendment were made to me in the course of consultation. One matching agency advocated the repeal of section 99(3), allowing for the charging of fees for services rendered, on the basis that the matter could simply be addressed between the parties. I take the view that section 99(3) needs to be retained. Without such a provision source agencies might be put in a difficult position in negotiating an agreement to recover their costs. Also, section 99(3) fees provide a convenient starting point, common to all matches, for the examination of the monetary costs of a match.

10.4.4 The other suggestion, made by more than one respondent to the information matching questionnaire, was that information matching agreements should be reviewed periodically by the parties to ensure that they remain relevant. The results should be reported to the Privacy Commissioner even if there is no resultant change to the agreement.⁴³



RECOMMENDATION 125

Section 99 should be amended to require the parties to review any information matching agreement at least once every three years and to report the results of that review to the Privacy Commissioner.

Downside

10.4.5 In some respects information matching agreements add a level of complexity, and potential for confusion, to the scheme provided by Part X and the Fourth Schedule. I expect that it has been intended that the information matching agreements particularise the requirements of the information matching rules and apply them clearly, and in appropriate detail, to the circumstances of a particular match. However, that has not always happened. Sometimes all that

⁴² See, for example, Privacy Act 1974 (USA), 5 USC §552a (o); Treasury Board of Canada Manual, Chapter 2.5 (Data Matching), page 8 (version 1 December 1993).

⁴³ If the agreement itself is changed this must already be copied to the Commissioner under section 99(4).

happens is that an agreement is prepared which paraphrases, and sometimes mis-states, the information matching rules.

- 10.4.6 I have not had sufficient resources to closely monitor the content of information matching agreements and indeed section 99 does not confer upon me any express function in that regard. However, on occasion my staff have compared the relevant clauses in agreements to the corresponding rules and found quite a casual translation of the obligations with, for example, “adverse action” being replaced with simple reference to “action” and “detected” overpayments substituted for “established” overpayments.
- 10.4.7 Even where confusion is not introduced by the substitution of imprecise or inappropriate terminology, the potential benefit of having an agreement is often not achieved. For example, one agreement refers to various obligations being placed with “either party” whereas it is presumably anticipated that an agreement should precisely identify the steps to be taken by, and obligations on, *each* agency.
- 10.4.8 The full potential for problems has not been realised yet due to the limited number of complaints.⁴⁴ I anticipate that there will be complexities uncovered in cases where an information matching agreement is claimed to be relevant in a complaint to an issue of compliance with Part X. It is essential that agencies appreciate the need for the agreements to be suitably detailed and particular.
- 10.4.9 I do not recommend that the role of the information matching agreement be dispensed with at this time. However, I do raise the possibility of problems and encourage specified agencies to give careful thought to the provisions in their information matching agreements. The provision for periodic review by agencies themselves may lead to an improvement in the position particularly as greater compliance experience is gained and shared between agencies. If resources were to be made available, it might be possible to undertake some work with agencies in developing a form of “model contract” which may be suitable for adaptation for particular programmes.

10.5 SECTION 100 - Use of results of information matching programme

- 10.5.1 This section provides that a specified agency that is involved in an authorised information matching programme may take adverse action, as defined in section 97, against an individual on the basis of results produced by that programme. However, this is subject to any other restrictions in law that limit or restrict the information that the agency may take into account in the circumstances.
- 10.5.2 A response to the questionnaire expressed concern that, as presently drafted, the section does not adequately limit who may use the results of an information matching programme. An example would be where a match has been established to enable agency A to take adverse action against individuals in respect of matters for which it is responsible. Agency A sends a list of its clients to agency B which carries out the process of comparison. Agency B returns the list of hits to agency A to enable adverse action to be taken. However, the concern expressed about section 100 was that agency B might not be precluded from itself using the results of the match for purposes of its own.
- 10.5.3 While the matter may not be as clear as might be desirable, I do not fully share the department’s concerns. Generally speaking present information matching

⁴⁴ Persons who have been matched are not usually told by agencies that they may complain to the Privacy Commissioner in the case of a breach of the information matching controls.

provisions have been written sufficiently precisely to make it quite clear what the purpose of the match is and which of the two agencies (or both) may make use of the results of the programme. While clarification would not do any harm, a change does not seem essential to achieve the desired end of constraining use of the results by agencies for which the information is not intended.

- 10.5.4 Section 100 uses the phrase “any specified agency that is involved in an authorised information matching programme”. At present, one cannot ascertain through the Privacy Act itself which agencies are actually involved in a particular programme. It may be that by listing specified agencies in the Schedule against the provisions which apply to them and by incorporating reference to “user agency”, which I have proposed be defined, the suggested problem could be addressed.⁴⁵ The proposed change would make the position plain, and constrain use, without the need to refer elsewhere to the information matching provision in question.

10.6 SECTION 101 - Further provisions relating to results of information matching programme

- 10.6.1 This section provides for certain restrictions on the right to use the results of an authorised information matching programme. Information produced by such a programme must be destroyed not later than 60 working days after the agency becomes aware of a discrepancy produced by the programme unless, before the expiration of that period, the agency decides to take adverse action against an individual on the basis of a discrepancy. Adverse action undertaken by an agency must be commenced not later than 12 months from the date on which the information was obtained by the agency. Where an agency decides not to take adverse action against an individual on the basis of the information produced by a programme, or where the information is no longer needed for such a purpose, the agency must destroy the information as soon as practicable.
- 10.6.2 Several comments in relation to this section were received in response to the questionnaire and discussion paper. It was suggested that the inter-relationship between the time limits in section 101 and information matching rule 6 regarding destruction of information could be better integrated. I suggest that consideration be given, when the information matching rules are more thoroughly revised, to consider how best this might be achieved.

Inland Revenue Department

- 10.6.3 Section 101(5) provides nothing in the section applies in relation to the IRD. Similarly, information matching rule 6(3) provides that nothing in that clause, which concerns destruction of information, applies in relation to the IRD. Accepting for the purposes of discussion that it necessary for IRD to be exempted, it does appear that the exemptions are drafted in a manner which may have a broader effect than was intended. I expect that it was intended that the exemption would apply where the information was supplied to IRD, or the “hits” were supplied to IRD, in order to allow IRD to take taxation-related adverse action against taxpayers. To use the terminology that I earlier proposed be introduced, I believe that the exemption was intended to apply to IRD where it is the authorised “user” agency.
- 10.6.4 I do not imagine that where (again to use the new terminology) a “source agency” supplies information to IRD to match, with the resultant hits being returned to the source agency as the “user agency”, that it was intended that IRD might also retain the list of hits on its records. Unless that is an intended effect of the programme then this should not be allowed to happen and IRD should not be able to use the exemption to permit it to retain the information. If IRD be-

⁴⁵ See recommendations 120 and 121.

believes that it legitimately should be able to use the particular information in the public interest then this should be written into the relevant information matching provision. Under the proposed terminology, IRD should be identified in such cases as a “user agency”.



RECOMMENDATION 126

Consideration should be given to limiting the Inland Revenue Department’s exemptions in section 101(5) and information matching rule 6(3) so that IRD is exempted from obligations to destroy information only where this is an intended objective of the programme.

10.7 SECTION 102 - Extension of time limit

10.7.1 This section provides that I may extend the 60 day time limit set out in section 101, if I am satisfied that the agency cannot reasonably be required to meet it because of the quantity of information obtained through the matching programme, the complexity of the issues involved or for any other reason.

10.7.2 In only one case has an extension of time been sought. The first attempt to run the IRD/DSW Commencement-cessation Match, formerly operated under section 13A of the Inland Revenue Act 1974, encountered difficulties in March 1993. In May 1993, DSW requested an extension of time under section 17 of the Privacy Commissioner Act 1991, the forerunner to section 102, to allow it to keep information generated by the March matching run which might otherwise have had to have been acted upon or destroyed within 60 working days. In the event, before the 60 day limit had expired and before I had made a decision upon the application for extension of time, DSW abandoned the March 1993 match results in the light of a decision to offer a benefit fraud amnesty.

10.7.3 A provision, such as section 102, conferring a discretion to extend time limits, remains desirable. The position seems more satisfactory from a privacy perspective than is the case in the Australian statutory data matching programme in which the relevant departmental Chief Executive can simply grant the extension.⁴⁶ It seems preferable that, if the time limits are to be meaningful, the occasional extensions which may be necessary should be the subject of an application to the independent Commissioner. Section 102 also appears preferable to the Australian approach in that it identifies reasons for which the Commissioner might grant an extension (albeit that the Commissioner can grant extension “for any other reason” in section 102(c)). The Australian provision gives no such guidance.

Which time limit?

10.7.4 One unsatisfactory aspect of section 102 is that it simply refers to extending “the *time limit* set out in section 101” whereas there are two time limits separately identified in that section. There is a 60 day time limit in section 101(1) and a 12 month limit in section 101(2). As mentioned, I have only ever received one application for an extension of the 60 day limit and, in fact, was not required to form an opinion on it. I have never been called upon to provide an extension in relation to the 12 month limit.

10.7.5 I note that section 102 was modelled upon section 10(3) of the Australian Data-matching Program (Assistance and Tax) Act 1990 (with the relevant provision now being contained in section 10(3A) by reason of a 1992 amendment). The Australian provision is directed solely towards the equivalent of the 12 month limit in section 101(2). This may be the period that the drafters of section 102 had in mind rather than the 60 day limit.

⁴⁶ Data-matching Program (Assistance and Tax) Act 1990, section 10(3A).

- 10.7.6 It seems desirable to amend section 102 to make the position plain. It may be desirable to allow the extension power to apply to both time limits even if it was originally only intended that extensions be able to be granted in respect of the 12 month limit. Given present experience, which suggests that applications will be rare, it seems desirable to allow the degree of flexibility that a broad extension power will bring. Nonetheless, I do see the extension power as being relevant to the exceptional cases and not as a means to routinely expand the time frames provided for in the legislation.



RECOMMENDATION 127

Section 102 should be amended to make clear that it refers to both the 60 working day time limit in section 101(1) and the 12 month time limit in section 101(2).

10.8 SECTION 103 - Notice of adverse action proposed

- 10.8.1 Section 103 provides that an agency may not take adverse action against an individual on the basis of a discrepancy produced by an authorised information matching programme, unless the agency has given that individual written notice of the particulars of the discrepancy. The agency must also provide details of the adverse action that it proposes to take and must allow the individual 5 working days from the receipt of the notice in which to show cause why the action should not be taken. There is also provision governing the circumstances in which the notice requirements may be dispensed with and concerning the deemed delivery of notices. The provision is modelled upon similar provisions in the Australian and American laws.⁴⁷

- 10.8.2 The period of notice in section 103(1) is 5 working days. This is provided in order to give the individual a chance to consider the matter and get in touch with the department to explain why it would be wrong to take adverse action. The period is not particularly generous to the individuals concerned and contrasts with the 28 day period (which translates to 20 working days) in the Australian Act.⁴⁸ The period initially specified in the Privacy of Information Bill was 15 working days, already a reduction upon the entitlement in the equivalent Australian legislation.⁴⁹ However, at Select Committee this was reduced to 5 working days. I am not satisfied that the reasons advanced in 1993 for doing so, such as a concern about departments being delayed in taking action, warranted the restriction. Nonetheless, I see no need to adopt a period as lengthy as exists in the Australian legislation. I take the view that 5 working days is too short and the protection of individual rights would be enhanced by modestly extending the period to 10 working days.



RECOMMENDATION 128

Section 103(1) should be amended by substituting a 10 working day period for the present 5 working day period.

Subsection (1A) - the Customs Match

- 10.8.3 Even before the Privacy Act 1993 had come into force it was subject to the Privacy Amendment Act 1993. This amendment inserted section 103(1A) which provides that in respect of the Customs Match the normal 5 day notice is not required. It is interesting to note that a match very similar to the Customs Match is currently being contested in a country sharing a number of values in common with our own. The following extract is taken directly from a recent annual report of the Privacy Commissioner of Canada:

⁴⁷ See Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 11, and the Privacy Act 1974 (USA), 5 USC §552a(p)(3) and (4).

⁴⁸ Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 11.

⁴⁹ Privacy of Information Bill, clause 104.

“Attention now turns to a practice which poses a deadly threat to privacy and to its corollary - autonomy and personal freedom. It has led us into a head-on collision with two great departments of government, HRDC⁵⁰ and Revenue Canada, precipitating a legal challenge which may ultimately determine whether privacy is a fundamental value of this society or merely an irritant quickly to be consigned to the scrap heap of unfulfilled good intentions when the going gets tough.

“That issue is data matching, an innocent-sounding activity with the capacity to demolish any real right to privacy and certainly to destroy the basis of trust which must exist between citizens who provide, and governments which collect, personal information.

“Given the intense pressure on government departments to be leaner (and, if necessary, meaner) coupled with the alluring ease of tracking citizens with computers, a confrontation was probably inevitable.

“At issue is HRDC’s practice of collecting data from the Customs declarations of every returning air traveller to identify employment insurance claimants who were out of the country while receiving benefits. EI⁵¹ claimants must report any extended absence from their normal residence for the good reason that they are expected to be looking, and available, for work. HRDC officials (and many taxpayers) have long been troubled by anecdotal evidence - approaching an urban legend - that many claimants were enjoying holidays at taxpayers’ expense. The department’s administration and enforcement methods were allegedly proving ineffective.

“HRDC conceived the notion of matching the EI database with that of returning travellers’ customs declarations. The match would quickly show whether any of those millions were receiving employment insurance payments. It would then be a simple matter to find whether they had reported their absences.

“Doubtless such a match will catch some who may be cheating EI. But the price it exacts is far too high. It systematically searches millions of innocent travellers, without their knowledge or consent, who filed customs returns on the assumption - and on Revenue Canada’s word - that they would be used for customs purposes only.

“The match offends the most fundamental principle of any privacy law; that government tell its citizens why it is collecting personal information, then use it only for that - and not a wholly unrelated - purpose (unless the individual consents). The reason for the principle is clear: to prevent the government from conducting unwarranted surveillance on its citizens by prowling through its immense personal databanks on what amounts to nothing more than high-tech fishing expeditions.



Bruce Slane and Bruce Phillips: The New Zealand and Canadian Privacy Commissioners confer at the 1998 Privacy Issues Forum.
PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

⁵⁰ Human Resources Development Canada.

⁵¹ Employment Insurance.

“Let us try a pre-computer age analogy. Assume there are some criminals at large in your community. Assume that the police therefore embark on a search of every single household, without warrant, without notice, without permission, and without any cause to suspect any particular household. The police just show up, barge through the door, and look around. How long would any community accept such arbitrary behaviour?”

“Yet, in an information context, that is precisely what data matching makes possible - a systematic search of everyone. Governments which match data this way have turned the presumption of innocence on its head; everyone is suspect until the computer proves them innocent. It is akin to what an earlier privacy commissioner described as ‘high technology search and seizure’. If we allow government to carry on in this fashion, they will routinely scrutinize every record of every citizen until they unearth some evidence of guilt.

“A privacy commissioner cannot accept a data search that ignores the presumption of innocence, the need to identify some reasonable grounds for suspicion, and the absence of independent authorization. If such matches become standard practice, we face virtually open season on any personal information we entrust, or are forced to deliver, to government.

“Unable to convince bureaucrats, or their ministers, to modify the match, we sought legal advice from one of Canada’s leading constitutional experts. His advice buttressed our position that the data match violates the search and seizure provisions of the *Canadian Charter of Rights and Freedoms*. We are currently exploring with the government the most expeditious manner of getting the matter before the Courts for resolution.

“No more crucial issue has arisen in my six years in this Office. I have no more interest in protecting [EI] cheats from detection than the next taxpayer. I have every interest in preventing government from putting millions of law-abiding Canadians under ‘dataveillance’. As a people and a society, we enjoy Charter protection against having to prove our innocence. One’s Charter rights should not be compromised simply because technology makes it possible.

“The premise of this match is boundless - once entrenched, we are on the slippery slope to a general surveillance system in which personal data from all levels of government are routinely shared and matched.”⁵²

- 10.8.4 I earlier noted that Part X has a role in *legitimising* data matching. It is in this context that I have my greatest concern with the Customs Match. Our present privacy law legitimises this programme and yet the Privacy Amendment Act 1993, which inserted subsection (1A) into section 103, undercuts the most fundamental of information matching safeguards - the presumption that the mere matching of information is not sufficient in itself to show guilt and that

⁵² Bruce Phillips, Privacy Commissioner of Canada, *Annual Report 1996-97*, pages 3-5.

the individual should be given an opportunity to explain themselves before adverse action is to be taken. I consider section 103(1A) to be an unjustified inroad into privacy safeguards which undermines the confidence the public ought otherwise to be entitled to have in respect of such an important matching programme.

- 10.8.5 Subsection (1A) also adds an unwelcome complication to the requirements of section 103. It has no application to most of the matches that are undertaken and, even if it were justified, the content of the subsection should really have appeared in section 280 of the Customs and Excise Act 1996. If it were relocated there the effect would substantively be the same but it would not result in clutter in the Privacy Act or confusion for other agencies.
- 10.8.6 However, relocation of the provision is not the best solution. It should, in my view, be totally repealed. It is objectionable in principle and has proved unnecessary in practice. When it was enacted in 1993 the Department of Social Welfare claimed that the amendment was urgent and essential to make the match effective. In fact, the Department has never used it and yet the match has been operated for a number of years. Years after the event, the Department may now wish to start relying upon it. This ought not to be permitted. Dispensing with the fundamental right to be notified of the proposed adverse action was never “essential”. This unjustified inroad into the scheme of information matching controls should be abolished.



RECOMMENDATION 129

Section 103(1A) should be repealed.

10.9 SECTION 104 - Reporting requirements

- 10.9.1 Section 104 provides that a specified agency that is involved in an authorised information matching programme must make certain reports to the Privacy Commissioner in respect of that programme, as may be required by the Commissioner from time to time.
- 10.9.2 In one sense the detail of section 104(2) is unimportant. This is because that subsection is not intended to limit the generality of section 104(1) which obliges agencies to make such reports as the Commissioner may require. However, section 104(2) is important as indicating Parliament’s expectations as to reports which might well be required. It provides a degree of guidance to the Commissioner and agencies. In particular, agencies can use section 104(2) as a guideline when planning the reporting capabilities of their information systems for a new programme.
- 10.9.3 In practically all cases to date it has been expected that agencies would report in the manner contemplated by section 104(2). This will not necessarily always be the case in the future. I would hope, after some years operation of any particular match, that a degree of comfort in relation to the issues addressed in section 104(2)(e) could be achieved allowing the adoption of less detailed reporting. I also hope to explore having departments undertake internal compliance audits with the results only reported to me rather than the “raw data” as contemplated by, say, section 104(2)(e). This comfort zone has not yet been reached with all matches I regret to say.

Australian equivalents

- 10.9.4 The detail of the provision has been derived from similar reporting requirements under the Australian Data-matching Program (Assistance and Tax) Act 1990. Specifically, the provision was modelled upon clause 9 of the schedule to that Act as it existed when the Privacy Commissioner Act was enacted in December 1991. The schedule to the Australian Act has since been supplanted by

a set of guidelines which have themselves been amended. The Australian Privacy Commissioner first issued guidelines pursuant to section 12 of the Australian Act in 1991. These replaced the schedule to the 1990 Act. The current Data-matching Program (Assistance and Tax) Guidelines were issued in 1994 and came into effect in early 1995.

- 10.9.5 The current guidelines do not appear to significantly differ from clause 9 although the following changes may be noted:
- the phrase “matches undertaken”, which is referred to in section 104(2)(e)(i) of our Act, has now been defined;⁵³
 - in relation to the material corresponding to section 104(2)(e) of our Act, the sub-paragraphs which refer to the “number of” items followed by, or preceded by, the “proportion of” such items, have been combined into composite “number and proportion of” provisions;
 - a reference to “successful recovery action” was replaced by a reference to “cases where the debt was fully recovered” perhaps to clarify what constitutes “success” - the nearest equivalent in our Act is section 104(2)(e)(viii) which refers to the number of “successful” cases but which, due to the broader coverage of the Act, is not described solely in terms of recovery action.
- 10.9.6 One of the responses to the questionnaire offered some criticisms of section 104(2)(e). The respondent pointed out, for example, the link between paragraphs (ii) and (iii), and (iv) and (v) which call for both figures and proportions while noting by contrast that (vi) and (viii) call only for a number and (vii) only for a percentage. The same respondent pointed out that (viii) refers to the number of cases - but not value - in which action taken was “successful”. It was suggested that value was important in constituting “success”. Consideration should be given to adopting some of the changes that have been made to the Australian provision from which section 104 has been derived. The Australian provision seems to have a more satisfactory current structure.



RECOMMENDATION 130

Consideration should be given to amending section 104(2)(e) to adopt aspects of the clause 12(v) of the Australian Data-matching Program (Assistance and Tax) Guidelines.

10.10 SECTION 105 - Information matching programmes to be reported on in annual report

- 10.10.1 Section 105 requires me to report on each authorised information matching programme in my annual report.
- 10.10.2 This has caused me some difficulties with completing my annual report, under section 24 of the Act, in time. I have been delayed in submitting my annual report because of the need to await departmental reports on the last matching runs held during any financial year in respect of particular information matching programmes. Consequently, the report on my activities tends to get held up which places me in the embarrassing position of failing to meet the timetable imposed by the Public Finance Act 1989 for the tendering of annual reports or failing to comply with this section. For example, in the 1996/97 year, final reports for four important matching programmes were only received by 22/23 September 1997.⁵⁴ In addition to the delay in completing the section 24 report, the need to finalise and submit my general annual report means that the

⁵³ Guidelines, clause 2.2(e). The definition is as follows: “**matches undertaken** refers to the total number of records received by the matching agency from assistance agencies after they have been separated into individual records for clients, partners, children, parents, maiden names and aliases.”

⁵⁴ These concerned the IRD/DSW Commencement/cessation match, Education/DSW match, Customs/DSW match and Corrections/DSW match.

report on information matching often has to be finalised in haste after the last departmental matching reports are to hand.

- 10.10.3 The two types of annual reports differ in nature and I believe there is a good case to split the reporting requirements. The section 24 report is an account of the activities of my office. The section 105 report is primarily, although not exclusively, a commentary upon the activities of other agencies. From a practical point of view, the completion of the section 24 report is within my own hands whereas I am dependent upon other departments to enable me to complete an adequate section 105 report.
- 10.10.4 I have considered several options for addressing the problem. The first would be to continue, as now, to try to reconcile the competing demands by allowing the section 24 report to be rather late and to complete the section 105 report as quickly as possible once the reports are to hand. However, this places me at risk in relation to compliance with the Public Finance Act. I have considered as an option whether to simply submit my annual report when the section 24 material and audited accounts are to hand, regardless of whether a complete set of departmental information matching reports are available to comment upon. I am reluctant to do this since it may mean that Parliamentary and public scrutiny of some of the matches, particularly those which have most difficulty in meeting section 104 reporting requirements, will be diminished. Furthermore, I am uncomfortable with failing to deliver a complete assessment of each information matching provision as anticipated by section 105. A third option was to adopt a different reporting year under section 105 to that used in the rest of my annual report and generally in the public sector. This would have the “information matching” year finish on, say, 31 December or 31 March. I concluded that this would be confusing.
- 10.10.5 Accordingly, I decided that the best way of resolving the problem will be to sever the section 105 report from the section 24 report. This will require section 105 to be amended since it anticipates the information matching report to be included “in every annual report of the Commissioner” which clearly refers to the section 24 report. Although I cannot be precise as to when an information matching report would likely appear each year I anticipate that it would usually be a few months after my general report. My annual report tends to be ready by about September each year and the information matching report could usually be ready by December. As with the present arrangement, I would wish the annual report to be tabled in Parliament since my recommendation is not intended to be a substantive change merely an alteration in timing and presentation. I suggest that the section merely provide that there be a report in terms of section 105 in respect of each year or, if it is desired to be more precise about the timing, that the report be submitted “as soon as practicable” following the completion of any year.



RECOMMENDATION 131

Section 105 should be amended so that the annual information matching report may be submitted separately from the annual report required under section 24.

Costs of monitoring and assessment

- 10.10.6 Section 105(3) provides that for the purpose of carrying out any assessment required to establish a programme’s compliance with Part X and the information matching rules that the provisions concerning complaints and investigations apply as if the assessment were an investigation under Part VIII of the Act. This anticipates more rigorous compliance assessments than has been possible for me to undertake to date. Primarily, the assessment that I have made to date have been done on the basis of an examination of the reports submitted to me under section 104 supplemented by specific correspondence. While I, and my staff, from time to time meet and talk with staff of agencies involved in infor-

mation matching I have not inspected premises with a view to making an assessment of the extent of any programme’s compliance.

- 10.10.7 This contrasts with the Australian Privacy Commissioner’s office which has been active in efforts to assess compliance. The Australian Commissioner’s Information Technology Standards Section monitors the statutory data matching programme by conducting audits of procedures and practices that are in place in the agencies.⁵⁵
- 10.10.8 The Act contains sufficient powers for me to undertake a more active role in this regard. Unfortunately, on present resources and particularly with the competing priority of a 12 month complaints queue, it has not been feasible to undertake such work. An independent oversight body in respect of data matching is intended to give the public, and affected individuals, some confidence that someone other than the agencies involved in the programme is ensuring compliance with the law. However, on present resourcing I fear that public confidence in the degree of oversight may be somewhat misplaced. This is compounded by the fact that reliance has been placed on the reports given to me under section 104 and experience has shown that the data contained in those has, in some cases, been wildly unreliable.
- 10.10.9 It may be appropriate to require specified agencies to fund the Privacy Commissioner to carry out aspects of this oversight role. This may seem appropriate for the following reasons:
- the extent of the work involved depends upon the number of new matches authorised and the amount of matching activity undertaken - the increase in the number of matches authorised has increased the work for my office;
 - enhanced activity by my office in respect of information matching will have a positive effect for agencies in helping them comply with the Act;
 - there is a benefit to specified agencies in being able to reassure the public that the process is carried out in the way which respects individual rights - the existence of independent oversight can help dispel public concerns about the process;
 - present arrangements mean that the cost of appropriate oversight are hidden, whereas it should be seen as one of the component costs of every authorised information matching programme.
- 10.10.10 My proposal has something of the “polluter pays” principle about it. The agencies which carry out the privacy intrusive process should bear the costs of the regulation which reassures the public, and Parliament, that citizens rights are being appropriately protected and the programmes are being carried out in the way that the legislation anticipates. This principle has already been accepted in Australia where the Commonwealth Department of Social Security provides funds to the Australian Privacy Commissioner for data matching regulation. The total amount received in 1996/97 was \$333,000.⁵⁶ If the Act adopts the concepts of “source agency”, “matching agency” and “user agency” it will be possible to most equitably allocate costs rather than levying all specified agencies equally. Costs would mainly be directed towards matching/user agencies.



RECOMMENDATION 132

Consideration should be given to funding the Privacy Commissioner’s information matching monitoring activities by charges on specified agencies involved in carrying out information matching programmes.

⁵⁵ See Australian Privacy Commissioner, *Ninth Annual Report*, 1996/97, page 102.

⁵⁶ *Ibid*, page 113.

10.11 SECTION 106 - Review of statutory authorities for information matching

10.11.1 Section 106 requires me at periodic intervals to review the operation of every information matching provision and to consider whether or not, in my opinion as Privacy Commissioner:

- the authority conferred by each information matching provision should be continued; and
- any amendments to the provision are necessary or desirable.

10.11.2 After a belated start, I have commenced work on this review. It has been necessary in 1998, as a matter of priorities, to delay completion of the first stage of the section 106 review as resources were deployed on completing this review. However, the section 106 review has progressed sufficiently such that the first part of that review should be complete at a time not too distant from the submission of this report.

10.11.3 If one considers the controls in Part X of the Privacy Act as following each part of an information match's life cycle the process might be characterised as:

- *authorisation* - the processes and controls which determine whether a proposed match should proceed and in what manner;
- *operation* - controls to ensure that privacy risks are minimised, decisions are based upon reliable information, individuals have an opportunity to explain themselves and if necessary complain, and independent oversight of the results of the programme;
- *evaluation* - periodic review of the continuing value of a match in the light of experience and current circumstances.

10.11.4 The section 106 review would encompass the third category. However, it would not be undertaken in isolation from the first two. In evaluating a programme I would look back to the objectives set, and projections made, when each programme was first authorised. I would also study the experience of each match in operation.

10.11.5 Notwithstanding the delay in completing the first batch of reviews expected under section 106, I consider the provision to be of significant importance in the scheme of information matching controls. No amendment to the section appears necessary although the matter could be considered again when the first reviews are complete.

10.12 SECTION 107 - Amendment of information matching rules

10.12.1 This section provides that the Governor-General, by Order in Council, may amend the information matching rules set out in the Fourth Schedule or may revoke the schedule and substitute a new schedule. No Order of this type may be made otherwise than in accordance with the recommendations of the Privacy Commissioner.

10.12.2 No Orders in Council have been made. I consider that the provision ought to be retained since proposals, when they arise, might be expected to be of a technical nature, rather than of a type raising important policy issues, and therefore better suited to regulations rather than requiring Parliamentary time. Nonetheless, there is an important safeguard in that no Order in Council may be made except in accordance with recommendations of the Commissioner. In the event that the Government wished to make a change which the Commissioner opposed, it would be possible for amending legislation to be brought to the House. Parliament would have an important role in respect of such a pro-

posed change. Most submissions saw the present process for amendment by Order in Council as satisfactory.⁵⁷

10.12.3 The information matching rules themselves are set out in the Fourth Schedule. I make some proposals for change to the rules which could be taken forward as part of any amending legislation arising from this report or separately by way of Order in Council. The changes that are proposed are relatively modest. A more thorough review of the information matching rules than has been possible on this occasion would be desirable with amendments made, as a result, by way of the section 107 process. This might usefully await the Government's responses to my recommendations for amendment to Part X. The Australian Privacy Commissioner has recently completed a revision of the relevant guidelines which may also present issues worth special consideration.⁵⁸

10.12.4 The changes to the information matching rules I suggest below are simply small technical changes which have been brought forward in the course of the review through responses to the information matching questionnaire, submissions on the discussion paper, or as suggestions from staff or agencies. They do not constitute a detailed reformulation of the rules and consideration has not been given at this stage to establishing any new rules. The changes therefore amount to refinement pending a more thorough review or reformulation at a later date.

Rule 1 - Notice to individual affected

10.12.5 Rule 1 obliges agencies involved in authorised programmes to take all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of it. This is quite different to the notice of adverse action to particular individuals whose information has been matched. Rule 1 requires specific classes of people to be made aware of the operation of a programme.

10.12.6 This requirement is a manifestation of the OECD "openness principle" which states:

"There should be a general policy of openness about development, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller".⁵⁹

It is a basic feature of privacy protection that there should be an openness about information use. This is particularly the case with information matching which is an intrusive process of mass "dataveillance" and which anticipates the use of information for a purpose other than that for which it was obtained.

10.12.7 In addition to the benefits for privacy from openness, there is in nearly all cases an incidental benefit to the primary purpose of matches. Many existing matches involve detecting unlawful behaviour. The government's interests will be better served if such wrongdoing is deterred in the first place. Deterrence ought to be underscored by fulsome compliance with information matching rule 1.

10.12.8 It is therefore disappointing to note that agencies have not been as active in

⁵⁷ Submissions PQ3, PQ4, PQ5 and PQ11 saw the process as satisfactory. PQ6 queried whether the process allowed sufficient consultation with affected government agencies while PQ8 considered the rules important enough to require statutory amendment in the rare circumstances that change were to be needed.

⁵⁸ See Australian Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration Guidelines*, February 1998.

⁵⁹ OECD Guidelines, clause 12.

"The use of an Order in Council to amend the privacy rules provides flexibility but also limits the opportunity for other government agencies to comment on the particular amendments. Legislating for changes to the Act provides a greater opportunity for comment."

- INLAND REVENUE DEPARTMENT,

SUBMISSION PQ6

their efforts to publicise the operation of matches as I believe is anticipated by rule 1. Only a few agencies have done a good job of publicising their programmes. Some others have made very expensive efforts from time to time, occasionally using television advertising, but have not sustained the effort at other times. In particular, the opportunities to communicate directly with beneficiaries, upon renewal or at regular intervals, should be taken as such efforts are better directed than mass media advertising.

- 10.12.9 When the information matching rules are more thoroughly revised I suggest that consideration be given to more fully articulating the steps which might be appropriate in notifying the commencement and the existence of a programme and generally making individuals aware of it. The Australian Privacy Commissioner's recently revised guidelines offer some suggestions for study in this regard.⁶⁰ I suggest that the phrase "openness and public awareness" appear in the heading so that agencies are directed to the purpose of the obligation.



RECOMMENDATION 133

Information matching rule 1 should be retitled "Openness and public awareness concerning operation of programme" and consideration should be given to enhancing the rule by detailing mandatory requirements, and a variety of discretionary methods, by which agencies may ensure that individuals who will be affected by a programme are made aware of its existence and effect.

Rule 2 - Use of unique identifiers

- 10.12.10 Rule 2 prohibits the use of unique identifiers in an information matching programme except as provided for in any other enactment or "unless their use is essential to the success of the programme." A perennial problem with information matching is to spot and ensure that the entries in two different databases indeed relate to one and the same individual. If the two sets of data which are to be matched in the programme both contain what should be the same unique identifier, then some would argue that its use may well aid in ensuring that it is the same individual in each database.
- 10.12.11 However, there are reasons which militate against the use of unique identifiers in information matching programmes. Experience has shown that unique identifiers which are held by an agency other than the one which assigned them are frequently incorrect. Thus when asked for their tax file number, some people will deliberately or mistakenly give a number which actually belongs to another member of their family or the agency may simply slip up in transposing the number from one form to another because there is no internal check on such identifiers and one identifier looks much like another. Reliance upon unique identifiers in such circumstances can reduce accuracy rather than increase it.
- 10.12.12 Another, and perhaps and even more compelling, reason for constraining the use of unique identifiers in information matching is the fear that if permitted to be used there will be a very strong incentive amongst Government bureaucracies to encourage the widescale use of shared unique identifiers. This in turn may lead to a national ID number to further facilitate widespread data linkages. Support for the view has been given by a policy decision to encourage the use of the driver licence for secondary purposes.
- 10.12.13 It should be noted that rule 2 is not an absolute prohibition on the use of unique identifiers. It is plain that unique identifiers can be used in two circumstances:
- where their use is provided for in another enactment; and
 - where their use is essential to the success of a programme.

⁶⁰ Australian Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration Guidelines*, February 1998, clauses 33-41.

In fact, unique identifiers feature in several existing information matching programmes.⁶¹

10.12.14 In practice to date, the information which is disclosed for an information matching programme has usually been detailed in the information matching provision. Thus rule 2 has not actually been an impediment to matching agencies so far so long as they can make a case for the unique identifier when they seek legislative authority. In the absence of legislative provision there seems to be no obvious way, short of seeking a declaratory judgment in the High Court, to establish whether or not an agency is correct in a claim that the use of a unique identifier is essential for the success of a programme. I expect that in case of disputes a department might seek to resolve such an issue by having an information matching provision amended to allow expressly for disclosure and use of the unique identifier.

10.12.15 However, it might be desirable to establish a process whereby an agency could apply to the Privacy Commissioner for approval to use a unique identifier where the Commissioner is of the opinion that the use of the identifier is essential to the success of the programme (or some other suitable or additional criterion). The power for the Commissioner to grant approvals under information matching rule 3 may offer a suitable precedent and such a power could provide that the Commissioner may impose conditions on the granting of such approval and may withdraw the approval or vary the conditions at any time. It might be appropriate for the Commissioner to limit approvals to cases where the unique identifier is one that is already assigned by the agencies so as to discourage the spread of common identifiers or the undermining of principle 12.

10.12.16 In the discussion paper I sought views on whether the use of unique identifiers should be permissible with the approval of the Privacy Commissioner. Although some of the replies were ambiguous it appears that nine submissions supported the proposition⁶² while three opposed it.⁶³



RECOMMENDATION 134

Information matching rule 2 should be amended by deleting the phrase “unless their use is essential to the success of the programme” and replace it with provision for agencies to apply to the Commissioner for approval to use unique identifiers where the Commissioner is satisfied that their use is essential to the success of the programme.

Rule 3 - On-line transfers

10.12.17 The prohibition on transfers by on-line computer connections has been derived from the Australian Data-matching Program (Assistance and Tax) Act 1990 which states:

“Data not to be sent on-line

Data is not to be transferred between agencies in the data matching program by on-line computer connections.”⁶⁴

10.12.18 I understand that this total prohibition has been controversial in data matching circles in Australia. Agencies involved would like to have the prohibition lifted and I understand that the Federal Privacy Commissioner has supported their case. However, Parliamentarians have been unwilling to allow that to happen and have apparently voted down a proposed amendment to lift the prohibi-

⁶¹ The tax file number is utilised in five information matching programmes. The Department of Social Welfare number and NZ Employment Service number are jointly utilised in a further match.

⁶² See submissions PQ1-PQ5, PQ7, PQ8, S36 and S42.

⁶³ See submissions PQ6, PQ11 and S45.

⁶⁴ Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 8.

“It will not be possible to use on-line transfers, which are prohibited under the rules. Nor will it be possible to establish a new databank for any matched information. The rules also require information that does not reveal a discrepancy to be destroyed forthwith. The Government is satisfied that this structure will provide the necessary safeguards.”

- HON. DOUGLAS GRAHAM, MINISTER OF JUSTICE, SPEAKING ON THE INTRODUCTION OF THE PRIVACY OF INFORMATION BILL, 1991

tion. It must therefore be acknowledged that at least in Australia there are strongly held views concerning the practice.

10.12.19 I suspect that the concerns exist on three levels. The first relates to the security of transmission of data. There are special information security issues about transfer of data by on-line computer connections but it appears that these are known and understood and able to be addressed. It is by no means certain that physical transportation of tapes and disks is invariably a more secure means of transfer. At the second level, the concerns relate to a fear of the inter-connection of a variety of Government databases. This raises the spectre of a “Government Super-computer” or “Big Brother” database which has been a recurrent public fear manifested in democratic societies. In New Zealand, similar concerns were at least part of the reason for the enactment of the Wanganui Computer Centre Act 1976. Finally, the third set of concerns relate to a worry that incorrect data from either agency be imported into records with insufficient checking in advance or ability to verify after the event.

10.12.20 In my view, there is a case to transfer data by means of on-line computer connections on occasion. Rule 3 is not the absolute prohibition that has been found to be problematic in the Australian legislation.⁶⁵ Agencies may obtain approval from me for on-line computer connections and in respect of one match I have granted such approval (on three separate occasions, the latest taking the approval through to 1 October 1998).⁶⁶ In my view, the rule at present continues to serve a useful function and contains sufficient flexibility to allow on-line computer connections in appropriate cases.

10.12.21 Further study could be given to dropping the prohibition when the rules are more fully reviewed. It may be that it should be replaced with a rule, or rules, specifically tailored to on-line issues. This may be especially desirable given that several of the rules have been originally drafted in Australia with only tape-to-tape matching in mind and may need to be modified to work well with on-line matching.

Rule 4 - Technical standards

10.12.22 There have been problems on occasion with agencies being unable to produce reports to the Privacy Commissioner of the type anticipated under section 104. The suggestion was made in a response to the questionnaire that it might be worthwhile to include in the rules a reference to adequate proposed procedures to generate, and supply, reports which may be required under section 104 by the Privacy Commissioner. Such an obligation would then have to be reflected in information matching agreements, pursuant to section 99 and the matter would therefore be one to which agencies will clearly turn their mind at an early stage and at a senior level. However, my recommendation to amend section 98(f) may diminish the problem and therefore I have not adopted this proposal.

Rule 5 - Safeguards for individuals affected by results of programmes

10.12.23 One respondent to the questionnaire echoed sentiments of others when he suggested that rule 5 was “difficult to understand, possibly ambiguous, and meriting review and revision”. One source of confusion are several difficult concepts such as:

- “the validity of discrepancies” - rule 5(1); and
- “the information which formed the basis for the information” - rule 5(3).

⁶⁵ When introduced in the Privacy of Information Bill did contain an absolute prohibition. The Select Committee introduced the power for the Commissioner to grant authorisations.

⁶⁶ See approval by the Privacy Commissioner under Information Matching Rule 3(1), 1 March 1998. This approval relates to a match operating between NZ Income Support and the NZ Employment Service.

“The other difficulty that I have is perhaps a rather strange one. We have to have a very careful discussion about the banning of on-line transfers, which are prohibited by the third information matching rule. I am not convinced that properly controlled on-line transfers are not a legitimate exercise in terms of, say, matching Department of Social Welfare and Inland Revenue Department data, because we will tend to end up with a much more expensive and highly complex set of manual information exchanges simply so that we can say that we are not having on-line transfers.”

- DR MICHAEL CULLEN, SPEAKING ON THE INTRODUCTION OF THE PRIVACY OF INFORMATION BILL, 1991

“Rule 7 is a valid precaution. Errors of mismatched information can have dire consequences and should not be used to form a new databank.”

- NZ ASSOCIATION OF SOCIAL WORKERS AOTEAROA, SUBMISSION
PQ 4

10.12.24 The origin of rule 5 is clauses 5.1 and 5.2 of the Schedule to the Australian Data-matching Program (Assistance and Tax) Act 1991.⁶⁷ However, the Australian provisions do not carry the two problematic phrases just mentioned. The manner in which they deal with the matter might suggest some ways forward to simplify the provision while retaining its effect. For example, in the Australian guidelines:

- the equivalent obligation to rule 5(1) applies to “source agencies” instead of, “the agencies involved in an authorised information matching programme” - there may be scope for simplification and precision through use of the new terminology suggested elsewhere;⁶⁸
- the phrase “source data”, a defined term, is used instead of “the information which formed the basis for the information” - which may be an approach able to taken up if the rules are used for defining terms as well as laying down rules, as recommended elsewhere;⁶⁹
- the phrase “believed that such results are not likely to be in error” is used instead of “confirming the validity of discrepancies” - I am not saying that one phrase is necessarily better than the other, simply that the Australian guidelines offer an alternative to consider.

10.12.25 The present heading for this clause is not particularly informative. It refers to “safeguards for individuals affected by results of programmes” which could just as easily refer to aspects of many of the other rules. Indeed, it appears that the adoption of that title may have been somewhat inadvertent when carried over from the Australian Act. The Australian Act uses “safeguards for individuals affected by the results of programmes” as a general heading which applies to the equivalent of rules 5, 6, and 7 of our Act. In fact, the precise heading applied to the equivalent of rule 5 in the Australian legislation is simply “fairness”. However, the way in which the heading and subheading are laid out in the Schedule to the Australian Act is confusing whereas the matter has been made much plainer in the Australian Privacy Commissioner’s guidelines. I suggest that a better heading should be adopted such as “procedures for confirming the validity of discrepancies” or “checking results before use”.



RECOMMENDATION 135

A more informative heading should be given to information matching rule 5 and consideration should be given to redrafting the rule in a clearer fashion possibly drawing upon the Australian approach and using defined terms.

Rule 6 - Destruction of information

10.12.26 Some aspects of this rule have been discussed already, at paragraphs 10.6.2 - 10.6.4, in relation to section 101.

Rule 7 - No new databank

10.12.27 One of the perceived dangers of information matching is that, unless action is taken to verify that an apparent match is a true match (that is, that the two records do in fact relate to the same individual), misinformation is generated and may potentially be used in the future upon the unwarranted assumption that the information is a historical fact. Rule 7 prohibits an agency from using the results of an authorised information matching programme to create a new databank and this might be thought primarily to ensure that the unverified information is not later treated as a fact.

10.12.28 It may also be the case that a match produces a “true match” of accurate information but nonetheless a permanent database of the information should not be

⁶⁷ Now contained in the Australian Privacy Commissioner’s Data-Matching Program (Assistance and Tax) Guidelines, clauses 5.1 and 5.2

⁶⁸ See recommendation 121.

⁶⁹ See recommendation 137.

retained. For example, if a superannuitant goes to Australia for a holiday that will be recorded as a departure. When he comes back after two months that is recorded as an arrival. He is within the permitted period of absence and no action needs to be taken. Nonetheless, through the operation of the information matching programme his details are identified. The Department has got the right person who did in fact do the things that the match identified. However, there was nothing wrong with it. It would seem unnecessary and improper to maintain a record of that permanently in Government files. Similarly, an unemployed person goes to Australia to seek a job. In fact she has the approval of the local Income Support office to do so. That record does not find its way through to the Head Office records by the time that the match is run. It is no doubt the right person identified in the particular case. A later investigation shows that she did have the necessary approval. Why should a record that she went to Australia and then came back again be maintained permanently? Accordingly, in addition to the concern about permanent records of misleading results, there is also a desire not to retain permanent databases of information for which no purpose, in terms of taking adverse action against the individual, exists.

- 10.12.29 The agency can keep a register showing those individuals in respect of which a “discrepancy” has been indicated by the matching programme but can only show the minimum details necessary for investigating and taking the adverse action against them. Similarly, the agency can keep a register showing individuals who are to be excluded from further investigation, but again just the minimum amount of information necessary for that purpose. These limitations do perhaps mean that extra work has to be undertaken in some matching programmes because intermediate match information which was not sufficient to warrant adverse action last time is lost and has to be produced again. On the other hand, one can argue that if the information was insufficient to warrant adverse action why should it be retained?
- 10.12.30 Some debate about rule 7 was engendered in the review process in the questionnaire responses and in submissions (for example, submission PQ 2). A suggestion was made to delete the word “permanent” from rule 7(1) and also the word “separate”. This would direct the rule towards avoiding creating new registers or databanks of information and not simply those that are separate or permanent. That idea may have merit but I prefer not to adopt it at this stage pending a more thorough review of the rules. Most submissions supported the rule as a safeguard.⁷⁰

Rule 8 - Time limits

- 10.12.31 I have observed elsewhere that the heading for this rule is somewhat misleading and suggest that it be retitled “Annual frequency of matches”.⁷¹
- 10.12.32 An interesting feature of this rule is that the time limits, or as I would characterise it the frequency of matches, are to be stated in writing in an annex to the Technical Standards Report. It is not plain why the frequency is required to be stated in an annex rather than the technical standards report itself. Indeed, a number of the Technical Standards Reports submitted to the Privacy Commissioner have not bothered to make the distinction. It may have been anticipated that the frequency of matching would likely have been a matter subject to change more frequently than the balance of the Technical Standards Report and that by dividing the material the documentation, and the management of change, may have been more easily handled. The Privacy Commissioner may pursuant to rule 4(6), require a change to a Technical Standards Report. Perhaps the annex was meant to be outside the scope of the Commissioner’s power to vary? If so, the effect is not plain.

“The no new databank rule may frustrate the objectives of matching programmes that have an intelligence gathering function but one can argue if the information was insufficient to warrant adverse action why should it be retained?”

- PAUL KELLY, SUBMISSION PQ2

⁷⁰ See submissions PQ1, PQ3-PQ5, PQ8, PQ11, S36 and S42. Submission PQ6 did not support the rule.

⁷¹ See recommendation 2.

- 10.12.33 In my view, the reason for specifying time limits in an annex is unclear both as to its purpose and effect. I suggest that the distinction be discontinued or, if on further study a good reason is ascertained, that the effect be more clearly spelt out.



RECOMMENDATION 136

Information matching rule 8(2) should be repealed or, if retained, its purpose and effect made plain.

Defining terms

- 10.12.34 The Fourth Schedule may have a useful role to play in defining technical terms which are used in the information matching rules or may be used in the future. However, it occurs to me that the process for amending the Fourth Schedule by Order in Council offers potential not only for defining terms used in the schedule but also for terms used in Part X. This would provide an appropriate way in the future of providing certainty on some legal, technical, and operational aspects without the need to await statutory amendment or to tie up Parliamentary time in enacting matters which may be highly technical.
- 10.12.35 I have seen an example of something similar happening in the Australian environment. Essentially the schedule to the Australian Data-matching Program (Assistance and Tax) Act has been replaced by a set of guidelines issued by the Privacy Commissioner. While the process differs from that provided in our Act, the nearest equivalent would be the issue of a substitute Fourth Schedule by Order in Council under section 107. Those guidelines introduced three new definitions which have not previously appeared in the Act: “Dispute”, “matches undertaken” and “final completion of the action”. “Matches undertaken” is a phrase used in Part X of our Act.
- 10.12.36 Without any amendment to section 107 it would be quite possible for newly issued information matching rules to contain a set of definitions of terms used in those rules. It would not be possible for the rules to define any term that is already defined in section 97 in a way that differs from section 97. Further, in the absence of a specific power to do so in section 97, it would be questionable as to whether the rules could purport to define a term used in both Part X and the rules (or if that was done, it would be unclear whether the definition was binding in respect of Part X itself) or used solely in Part X (which would be highly doubtful). I suspect that, if the Order in Council procedure is to have most value as a definitional aid, section 97 or section 107, or both, should be amended to expressly so provide. The basic power could perhaps be provided in section 107 with section 97 appropriately amended to make clear that any terms not defined in section 97 itself to have the meaning ascribed by definitions (if any) in the information matching rules.



RECOMMENDATION 137

Provision should be made for terms used in Part X, and the information matching rules, to be able to be defined in the information matching rules themselves.

10.13 SECTION 108 - Avoidance of controls on information matching through use of exceptions

- 10.13.1 Section 108 provides that nothing in information privacy principles 2(2)(d)(i) or 11(e)(i), which allow a public sector agency to collect or disclose personal information in order to avoid prejudice to the maintenance of the law, permit the agency to collect or disclose that information for the purposes of any authorised information matching programme, or any information matching programme the object of which is similar in nature to any authorised information matching programme.

- 10.13.2 Where there is a specific statutory arrangement for matching under an information matching provision listed in the Third Schedule, the exceptions to principles 2 and 11 in relation to the maintenance of the law cannot be invoked in order to avoid the controls placed on the authorised information matching programme by Part X. The purpose of section 108 is to counteract a means by which public sector agencies might otherwise be able to circumvent the controls on information matching.
- 10.13.3 Clearly the exceptions to principles 2 and 11 mentioned in the section are the most likely to have been cited in the event that section 108 had not existed. However, they are not the only ones and there is now a broader range of programmes that have been authorised than was the case when section 108 was enacted. For example, there is a match authorised involving the Department for Courts designed to obtain new address information to enable the Department to enforce fines. The harm to which section 108 is directed would also exist if such a department could skirt the information matching controls by reliance upon principle 2(2)(d)(ii) or principle 11(e)(ii) rather than the subparagraphs presently mentioned in the section. The Australian Privacy Commissioner, who has a similarly worded disclosure principle, has also expressed concern at the use of such exceptions to legitimise bulk disclosures for data matching exercises.⁷²
- 10.13.4 Accordingly, I suggest that section 108 be amended to refer to all of the exceptions appearing in information privacy principles 2 and 11.

**RECOMMENDATION 138**

Section 108 should be amended to replace the reference to “subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11” with a reference to all of the exceptions to principles 2 and 11.

10.14 SECTION 109 - Avoidance of controls on information matching through use of official information statutes

- 10.14.1 Section 109 provides that a public sector agency is not to disclose personal information in response to a request made by another public sector agency under either of the official information statutes where the sole or principal purpose for the request of the information is so that it may be used in an information matching programme.
- 10.14.2 The purpose of section 109, like section 108, is to counteract a means by which public sector agencies might otherwise be able to circumvent the controls on information matching provided for in Part X. However, section 109 goes beyond section 108 in applying to all information matching programmes, not just authorised information matching programmes or programmes which are similar in nature to an authorised information matching programme.

⁷² Australian Privacy Commissioner, Privacy Protection in the Private Sector: Response to Discussion Paper issued by the Attorney-General, December 1996, page 9.

