

Part XII

XII

Miscellaneous Provisions

349

“I have no doubt that the intention of the Wanganui Computer Centre Act was simply to enable the public to check for themselves whether the official record was correct as far as they were concerned. It exceeds the legislative purpose if pressure is brought to bear on members of the public to supply information from the database that is and always was intended to be confidential as far as possible.”

- P L Molineaux, *Report of the Wanganui Computer Centre Privacy Commissioner*, 1987

“You questioned whether it is appropriate to create an offence of misleading an agency in order to gain access to information, either by impersonating the individual concerned or misrepresenting that they have an authorisation from that person. You also suggested that there might be an offence of knowingly destroying information to which a person is entitled in order to deny the person access to it. In both of these instances you note the Privacy Act obliges agencies to open their files to individuals where previously they may have kept them far more securely closed to outsiders, and that the agency and the individual are at risk. It would not be inappropriate to incorporate an offence provision in these circumstances. Obviously an eye would need to be kept on whether it is appropriate to invoke the sanctions of the criminal law in what is essentially a civil context. In our view the examples you give are appropriate ones”.

- Crown Law Office, submission G16

“The issue of computer crimes is one that needs to be addressed with some urgency. The Group does not, however, consider that the Privacy Act is the appropriate vehicle for addressing the issue.”

- NZ Law Society Privacy Working Group, submission G22

12.1 INTRODUCTION

12.1.1 Part XII brings together a series of unrelated provisions.

12.1.2 The provisions are grouped into six categories:

- general - sections 115 to 120;
- delegations - sections 121 to 125;
- liability and offences - sections 126 and 127;
- regulations - section 128;
- amendments, repeals and revocations - section 129;
- transition provisions and savings - 130 to 133.

SECTION BY SECTION DISCUSSION

12.2 SECTION 115 - Protection against certain actions

12.2.1 Section 115 protects requesters and providers of personal information, as well as others, from legal liability arising from the mere use of, or compliance with, the Act. These immunities are limited to actions taken in good faith pursuant to information privacy principle 6. The section is derived from section 48 of the Official Information Act 1982, as inserted in 1987. The drafting of the original section 48 of the Official Information Act was deficient and the 1987 provision was intended to remedy those deficiencies.¹ However, commentators on the Official Information Act have suggested that there remains a drafting deficiency with section 48 - and hence section 115 of the Act.

12.2.2 The issues have been described by Dr Paul Roth in *Privacy Law and Practice* as follows:

“A comparison of subs(1)(a) and (b) with subs(2), might suggest that there is some significance to the distinction drawn between ‘the making available of [personal] information’ on the one hand, and ‘the making available of, or the giving of access to, any personal information’ on the other. A similar distinction is drawn in both s.48 of the OI Act and s.41 of the LGOIM Act. Elsewhere in the OI Act a distinction is indeed maintained in relation to information to which there is a right of process (Part II, dealing with official information in the general sense) which is made available, and information to which there is a right of access (Part III and IV, dealing with certain forms of official information and personal information) to which access is given. However, it is unlikely that this subtle distinction would have any significance in regard to the immunities conferred by the relevant legislation. Accordingly, the distinction in s.48 of the OI Act (and carried over into subsequent freedom of information legislation) has been suggested to be an oversight in drafting: see I Eagles, M Taggart, G Liddell *Freedom of Information* (Auckland, 1992), p 614.”²

12.2.3 Dr Roth notes that this particular issue was expressly considered by the Select Committee which studied the Privacy of Information Bill. He states:

“The distinction was noted in the report of the Department of Justice to the Privacy of Information Sub-Committee of the Justice and Law Reform Committee (22 January 1993, p30), which commented that explicit limitations of the section to principle 6 would make it clear that the section was based on, and thus should have the same construction as, s.48 of the OI Act.”³

12.2.4 Given that the select committee had the issue drawn to its attention, took advice and made an informed decision about the drafting, the matter could be left there. Indeed, I am unaware that the issue has caused any difficulties. However, it must be borne in mind that the select committee had before it only the privacy legislation. It could not, of course, have amended the Official Information Act. Therefore, if the Privacy of Information Bill had struck out in a new

¹ Section 48, and its original deficiencies, are discussed in *Freedom of Information in New Zealand*, pages 613-614.

² *Privacy Law & Practice*, paragraph 1115.4.

³ *Privacy Law & Practice*, paragraph 1115.4.

direction it would quite possibly have caused new difficulties of interpretation and consistency. However, we are now at a point whereby further consideration could be given to this issue so that, if appropriate, a consistent amendment could be made to each of the Privacy Act, Official Information Act, and Local Government Official Information and Meetings Act.



RECOMMENDATION 143

Consideration should be given to the merits of making consistent amendments to:

(a) section 115 of the Act;

(b) section 48 of the Official Information Act 1982; and

(c) section 41 of the Local Government Official Information and Meetings Act 1987;

to meet the perceived difficulties of interpretation raised by the distinction in the first and second subsections of each of these provisions between “the making available of information” and the “making available of, or the giving of access to, information”.

12.3 SECTION 116 - Commissioner and staff to maintain secrecy

12.3.1 This section requires:

- the Commissioner; and
- every person engaged or employed in connection with the work of the Commissioner;

to maintain secrecy in respect of all matters that come to those persons' knowledge in the exercise of their functions under the Act. However, as Commissioner, I may disclose such matters as in my opinion ought to be disclosed for the purposes of giving effect to the Act - but this does not extend to information that might prejudice certain listed public interests such as national security and cabinet confidences.

12.3.2 The provision is necessary since a variety of material which must remain secret is brought into my office pursuant to a variety of my functions, especially my investigative functions.⁴ For example, I may at any time be holding thousands of copy documents which are being reviewed to see whether the agencies that hold them should release the material to requesters. I am subject to both the Official Information Act and the rights of access conferred by information privacy principle 6, but it would undermine the review process if such documentation could be sought directly from me. The secrecy obligation goes beyond the circumstances where I might receive a request or demand for information and also constrains my own disclosure of certain sensitive information.

12.3.3 Naturally a secrecy obligation of the type imposed by section 116 needs, to be effective, to also apply to former staff, consultants and commissioners, after they leave the office. I expect that this section, and section 96 to which it is linked, may be open to be construed so as to apply to former staff. However, it does not say so explicitly. By contrast the Serious Fraud Office Act 1990, which has a secrecy provision similar to section 116 (section 36), also has a section imposing a continuing obligation in respect of persons ceasing to be members of the Serious Fraud Office (section 44).

12.3.4 The Australian Privacy Act's secrecy provision applies to:

“a person who is, or has at any time been, the Commissioner or a member of staff or is acting, or has at any time acted, on behalf of the Commissioner.”⁵

12.3.5 It would seem desirable to make the position explicit. To avoid cluttering the Act with a new section modelled upon section 44 of the Serious Fraud Office

⁴ Privacy Act, section 90(1), makes clear that every investigation is to be carried out in private.

⁵ Privacy Act 1988 (Australia), section 96(1).

Act, I suggest that section 96(1) be amended or that a new provision appear in the First Schedule.



RECOMMENDATION 144

Section 96, or the First Schedule, should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner.

12.4 SECTION 117 - Consultation with Ombudsmen

12.4.1 One of the consequences of having a secrecy provision like section 116, is that it becomes desirable for further provisions to outline the circumstances in which otherwise secret information can be disclosed. Section 117 is such a provision which provides the authority for sharing information with an Ombudsman during consultations. However, the secrecy provision is only one reason for having consultation provisions. They are also intended to foster co-operation and avoidance of duplication of work. The Ombudsmen, and their office, are an important part of the fabric of the public sector in New Zealand. I have valued the discussions that I have had with the present and former Ombudsmen.

12.4.2 The first type of consultation anticipated in paragraph (a) involves the making of a determination under section 72 - that is, the referral of a complaint to an Ombudsman where that complaint more properly comes within the jurisdiction of the Ombudsmen. Under paragraph (b) I may consult in relation to any matter arising in the course of an investigation under Part VIII of the Act. Such consultations are particularly valuable where there is:

- in the subject matter of the complaint, an inter-relationship between the Privacy Act and the official information legislation;
- an investigation also being undertaken by the Ombudsmen under the official information legislation or the Ombudsmen Act, or it might be desirable for there to be such an investigation.

12.4.3 Paragraph (c) anticipates consultation on matters relating to privacy whether or not a complaint has been lodged. Although not as frequent as the other consultations, these do occur from time to time as it is desirable for the Commissioner and Ombudsmen to be aware of each other's views on such matters. A recent example would be some general consultations, which have flowed from, but are not directly related to, the privacy and administrative issues arising in relation to adoption information and the interests of adopted persons, birth mothers, adoptive parents and the descendants and siblings of the various parties.

12.4.4 The other consultations held with the Ombudsmen arise pursuant to sections 29B of the Official Information Act 1982 and section 29A of the Local Government Official Information and Meetings Act 1987. These oblige the Ombudsmen to consult with the Privacy Commissioner when reviewing a decision to withhold information on a complaint under that legislation before forming a final opinion in relation to the merits of refusing a request on grounds related to privacy. I have considered these consultations to be of particular importance amongst the functions I carry out arising in relation to other enactments. I have seen it as important to be personally involved in each such consultation although this involves a not inconsiderable commitment of time and resource.

12.4.5 The following table gives the number of formal consultations with the Ombudsmen under the official information statutes recorded since 1993:

FIGURE 4. OMBUDSMEN CONSULTATIONS				
1993/94	1994/95	1995/96	1996/97	1997/98
22	26	60	87	77



12.5 SECTION 117A - Consultation with Health and Disability Commissioner

12.5.1 Section 117A was inserted by section 81(2) of the Health and Disability Commissioner Act 1994 with effect from 20 October 1994. There have been fewer formal consultations with the Health and Disability Commissioner compared with those undertaken with the Ombudsmen. The provision is not in need of amendment.

12.6 SECTION 117B - Consultation with Inspector-General of Intelligence and Security

12.6.1 Section 117B providing for consultation with the Inspector-General of Intelligence and Security was inserted in 1996. I supported the inclusion of the provision in my report on the Intelligence and Security Agencies Bill.⁶ As with the other consultation provisions, the section marks out the point of interaction between our respective functions, encourages consultation in matters affecting both offices, and provides authority for necessary disclosure of confidential information in the course of those consultations.

12.6.2 I have concluded that it would be desirable to create a single generic consultation provision which would combine sections 117, 117A and 117B and provide a framework for the addition of any further statutory bodies which require to be listed. It may even be desirable to remove the detail of the types of consultations to a new schedule. This would have two columns. The first would indicate the officer with whom the Commissioner would undertake consultation with the second modelled upon items (a) to (c) of sections 117, 117A and 117B.



RECOMMENDATION 145

Sections 117, 117A and 117B should be combined into a single consultation section with consideration given to placing the details of the officer with whom consultation is to be undertaken and the purposes of such consultation in a new schedule.

12.6.3 I have considered the merits of including consultation provisions with other statutory bodies. One such statutory body, subject to a secrecy provision, which would seem to be an appropriate candidate is the Police Complaints Authority.⁷ Others would include the Human Rights Commission and Broadcasting Standards Authority.



RECOMMENDATION 146

Consideration should be given to making provision, along the lines of sections 117 to 117B, for consultation with other statutory bodies such as the Police Complaints Authority.

12.7 SECTION 118 - Corrupt use of official information

12.7.1 Under section 118:

- the Privacy Commissioner; and
- every person engaged or employed in connection with the work of the Commissioner;

are deemed to be “officials” for the purposes of sections 105 and 105A of the Crimes Act 1951 which provides for the prosecution for the corrupt use of official information or the use of personal information disclosed corruptly. This

⁶ Report by the Privacy Commissioner to the Minister of Justice on the Intelligence and Security Agencies Bill, 26 February 1996.

⁷ The relevant secrecy provision is Police Complaints Authority Act 1988, section 32.

is a standard provision in legislation which creates new public entities to ensure that the bribery and corruption laws effectively extend to the new bodies.

- 12.7.2 Section 105B of the Crimes Act 1961 exists to make unlawful the trade in corruptly disclosed personal information. Section 105B was, on my suggestion, inserted into the Crimes Act in 1993 on the recommendation of the committee which studied the Privacy of Information Bill.
- 12.7.3 I supported the enactment of section 105B which implemented a recommendation of the New South Wales Independent Commission against Corruption (ICAC) which had just completed a major study into the trade in corruptly disclosed government information.⁸ What was uncovered by ICAC in New South Wales was a disturbing trade in which officials were being paid to release government information - usually to private investigators. In many cases the private investigators were procuring the information for reputable organisations, like banks and insurance companies, which sometimes even directed which Government database was likely to hold the information sought. Existing law in New Zealand, and no doubt New South Wales, was effective to criminalise the actions of the officials who corruptly disclosed the information, and the private investigators who bribed those officials. However, the trade continued to flourish because a market existed. Section 105B is intended to make it clear that anyone who knowingly uses such corruptly obtained information will themselves commit an offence.
- 12.7.4 When the opportunity arose in 1994, I recommended that amendments be made to the Private Investigators and Security Guards Act 1975 so that a person who has been convicted of an offence under section 105B should be barred from being licensed as a private investigator.⁹ I made this recommendation on the basis that ICAC evidence showed that private investigators were, in nearly all cases, the “middle men” who procured the corrupt release of official information and enabled the trade to flourish. I am pleased to say that reference to section 105B was made.¹⁰

12.8 SECTION 119 - Exclusion of public interest immunity

- 12.8.1 Section 119 prevents claims of public interest immunity, in order to exclude evidence, from arising in investigations by the Privacy Commissioner, proceedings before the Complaints Review Tribunal, or in judicial review proceedings. However, this exclusion does not give anyone an additional right to obtain information that they would otherwise not have.
- 12.8.2 The provision is derived from section 11 of the Official Information Act 1982. In discussion of that provision it is noted in *Freedom of Information in New Zealand* that:

“The Act strengthens the courts’ hand in reviewing decisions under the OIA by excluding claims of public interest immunity. However, the draftsperson was obviously concerned that an unsuccessful complainant before the Ombudsman might take advantage of this and initiate review proceedings as an indirect means of obtaining information which is protected by the Act. To prevent this occurring the following words were added to section 11(1): ‘but not

⁸ Independent Commission against Corruption, *Report on Unauthorised Release of Government Information* (3 volumes), August 1992.

⁹ See Report of the Privacy Commissioner to the Minister of Justice on the Law Reform (Miscellaneous Provisions) (No 3) Bill, October 1994.

¹⁰ See Private Investigators and Security Guards Act 1975, section 17.

so as to give any party any information that he would not, apart from this section, be entitled to’.

“Taken as a whole, section 11 seems to envisage that the court will examine the withheld material *in camera* with a view to acting on it as evidence even though it will be kept from the requesting party during the proceedings. While, generally speaking, it is undesirable and almost certainly unlawful for a court to rely on evidence that one side has not seen, this practice appears to be sanctioned by section 11(1) and is necessary to ensure that all the relevant information is put before the court without defeating the purpose of withholding information in the first place.”¹¹

- 12.8.3 As an aside, and unconnected with section 119, there has been a Complaints Review Tribunal case in which evidence was heard by the Tribunal *in camera* in the absence of the plaintiff. In *O v N (No 2)*¹² the plaintiff was seeking the identity of “X” referred to in a psychologist’s report. To assist the Tribunal I made the suggestion, which was acted upon, that the Tribunal should initially consider whether there was good reason under section 29(1)(b) to withhold information before seeking information as to who X was. If it had been held that there was good reason to withhold then the problem of how to receive evidence from or about X, without disclosing material tending to identify X to the plaintiff, could be avoided.
- 12.8.4 In fact, the Tribunal determined that it was necessary to consider evidence of X’s identity and therefore developed a means for hearing the evidence. The Tribunal developed a draft practice note based upon the practice of the Australian Administrative Appeals Tribunal which it provided to the parties for comment. Later the Tribunal convened a hearing in the absence of the plaintiff and the plaintiff’s representative to hear from the Commissioner’s counsel about what the Commissioner knew of X and why the Commissioner was of the opinion that X’s name should be withheld. The Tribunal considered that information and ruled in the plaintiff’s presence that the hearing would be adjourned for the rest of the day and that it would receive evidence from X in the plaintiff’s absence. The evidence was received in the presence of the Commissioner’s counsel.

12.9 SECTION 120 - Adverse comment

- 12.9.1 This provision requires the Commissioner, when proposing to make a comment that is adverse to another person, to give the person concerned a chance to present his or her side of the matter. The provision is derived from section 78(2) of the (now repealed) Human Rights Commission Act 1977 and continues section 32 of the Privacy Commissioner Act 1991.
- 12.9.2 The provision has its main relevance in respect of my functions in relation to complaints although it occasionally arises in other contexts as well.¹³ The practice I have adopted in relation to complaints which have not proved possible to settle is to write a provisional opinion which is given to the party to which it is adverse. That party is given a reasonable opportunity to respond and, if the complaint is not settled in the meantime, I either confirm my opinion as final or reconsider it in the light of representations made. In fact, because of the nature of the jurisdiction, I commonly render opinions which are adverse in

¹¹ *Freedom of Information in New Zealand*, 1992, page 594.

¹² (1996) 3 HRNZ 636

¹³ I have for example sometimes shown drafts of reports, or public statements, that I have intended to make to certain parties in this vein.

some respect to one party yet favourable in another. This is particularly the case where a complaint raises issues under several information privacy principles or where several grounds are relied upon to withhold information. In such cases a provisional opinion, in different terms, is rendered to each party.

- 12.9.3 The complaints process itself is an inquisitorial one and the *audi alteram partem* rule does not apply. It is therefore important that the party has an opportunity to comment, not during the process of investigation, but at the point when the Commissioner is about to come to an opinion. The procedure is adopted because of its advantages to the investigation in ensuring that each party's position has been understood and that the provisional interpretation of the facts by the Commissioner can be addressed.

12.10 SECTION 121 - Delegation of functions or powers of Commissioner

- 12.10.1 The section permits me to delegate to any person holding office under me any of my functions or powers under the Act or under any other Act.

- 12.10.2 In practice I have been sparing in my use of the delegation power. While I have, for instance, delegated the function of rendering opinions on complaints to my Manager Investigations, the power is not generally exercised except when I am unable to fulfil the function personally - for example, where I am out of the country or there may be a perceived conflict of interest.¹⁴ I am satisfied that much of the fine reputation of the Ombudsmen was built on the knowledge that the decisions made were those of the Ombudsmen themselves. Likewise I believe that confidence in the opinions I give may often be derived from the fact that the opinion is that of the Commissioner and not of a deputy or a delegate. Also I have taken the view that in the early years of the Act it is expected that I, as Commissioner, personally give opinions on complaints which may act as precedents (in a general - not legal - sense) for both my office and for agencies. I appreciate with the increase in the volume of complaints a different view may be taken in the future and the Commissioner may delegate the rendering of opinions on certain classes of complaints.

12.11 SECTION 122 - Delegate to produce evidence of authority

- 12.11.1 This provision requires that a delegate of the Commissioner produce evidence, when required to do so, of that person's authority to exercise the Privacy Commissioner's power. This has not caused any difficulties in practice.

12.12 SECTION 123 - Revocation of delegations

- 12.12.1 Section 123 provides that every delegation under section 121 is revocable, at will, in writing. The delegation is to continue in force until revoked, even if the Commissioner who originally made the delegation no longer holds office. No issues have arisen in practice as yet.

12.13 SECTION 124 - Delegation of powers by local authority

- 12.13.1 Sections 124 and 125, which run to almost two pages of the statute, concern delegation of powers by local authorities and by officers of local authorities. In 1997 it was suggested to me that these provisions were unnecessary due to sufficient powers of delegation existing in the Local Government Act 1974. I determined to follow through on this issue since there appeared to me to be an opportunity to "unclutter" the Act if these two lengthy provisions could be omitted. In the discussion paper I posed questions to find out whether local

¹⁴ For example, where a respondent was a company of which I had previously been a director.

authorities considered sections 124 and 125 really necessary or whether they would find it more convenient to have the delegation powers located in the Local Government Act.

12.13.2 In addition to receiving submissions from local authorities, and people knowledgeable about local authority affairs, I invited representatives from local authorities in the Wellington and surrounding regions, Local Government New Zealand and the Department of Internal Affairs to a meeting in December 1997. I obtained a number of valuable comments. A consensus was reached that territorial authorities would find it advantageous to use the delegation powers in the Local Government Act since this is their normal point of reference. Another advantage of repositioning delegation powers is that the Local Government Act establishes a delegation register which is a valuable central reference point. Delegation powers become problematic when they are scattered throughout other pieces of legislation.

12.13.3 Local authorities present at the meeting suggested that section 78 of the Building Act 1991 provided a model for a replacement to sections 124 and 125. That section provides:

“Delegation of powers by territorial authority and its officers - The provisions of sections 715 and 716 of the Local Government Act 1974, with all necessary modifications, shall apply in respect of the powers under this Act of every territorial authority and its officers.”

12.13.4 A provision to replace sections 124 and 125 of the Act, modelled upon section 78 of the Building Act, might appear something like the following:

Delegation of powers by local authority and its officers

- (1) The provisions of sections 715 and 716 of the Local Government Act 1974 apply in respect of the powers under this Act of every local authority that is a council, within the meaning of that Act, and of members and officers of the council.
- (2) The provisions of sections 42 and 43 of the Local Government Official Information and Meetings Act 1987 apply in respect of the delegation of the powers under this Act of every local authority not specified in subsection (1) and of officers and employees of the local authority.

12.13.5 The draft provision is more complex than section 78 of the Building Act as it needs to take account of the fact that not all “local authorities” are “territorial authorities” subject to the Local Government Act. However, those other local authorities are satisfactorily accounted for in the proposed subclause (2).



RECOMMENDATION 147:

Sections 124 and 125 should be repealed and replaced by a single brief provision providing that the relevant delegation provisions in the Local Government Act 1974 and Local Government Official Information and Meetings Act 1987 apply.

12.14 SECTION 125 - Delegation of powers by officers of local authority

12.14.1 Section 125 provides that any officer or employee of a local authority may, by writing, delegate to any other officer or employee any of his or her powers under the Privacy Act, except the power to delegate under section 125 itself. As discussed in relation to section 124, involving delegation of powers by a local

XIII

s 125

357

“Sections 124 and 125 of the Privacy Act are almost identical to the general delegation power under the Local Government Act 1974. Having separate provisions is confusing. We suggest their replacement by a reference to the Local Government Act. (This will have the added benefit of bringing the Privacy Act delegations within the ambit of the delegations register).”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

authority, I believe that this provision may be more briefly stated and the details should primarily be found in local government statutes.

12.15 SECTION 126 - Liability of employer and principals

- 12.15.1 I have already briefly mentioned this provision in the context of section 4 which concerns the actions of, and disclosure of information to staff of an agency.¹⁵ I observed that it is unfortunate that it is necessary for employers and employees to seek out sections in opposite ends of the statute to obtain the complete picture on liability. However, I took the view that if each provision is read a reader will obtain a relatively plain message as to the combined effect.
- 12.15.2 I have had to consider section 126 in a number of cases. In respect of several of these I have issued case notes.¹⁶ The Tribunal has not yet given a decision concerning the interpretation of the provisions. I have no recommendation to change the section.

12.16 SECTION 127 - Offences

- 12.16.1 Unlike many overseas privacy laws, there are very few criminal offences in the Privacy Act. For example, it is not an offence to breach an information privacy principle. Rather, the Act provides for civil remedies. If an agency has caused an interference with the privacy of an individual the Act can provide a resolution to an individual's complaint and, if necessary, compensation or enforceable orders to prevent repetition of the harm. I prefer this approach to any widespread use of the criminal law which would seek to punish an agency. Both approaches are directed towards preventing a repetition of the action but the civil law approach is less "heavy handed" and ensures that the individual, who should be the centre of any privacy process, is given redress if possible. I am not persuaded that it would generally be better to enforce the privacy principles by criminal law sanctions. The purpose of the Act is to improve agencies' practices in respect to personal information. The efficacy of the criminal law approach in this regard is suspect. Indeed, the imposition of criminal liability on such parties can be counter-productive.
- 12.16.2 However, it is appropriate to supplement with certain offence provisions a law which primarily revolves around civil law remedies. An example of this is the existing section 127 which provides for a fine of up to \$2,000 for deliberately obstructing or misleading the Commissioner. I believe that the addition of some further and suitably crafted offences will make the legislation more effective. However, I have been cautious in recommending such measures since I continue to believe that the present civil approach continues to be the most appropriate. The recommendations I make for new offences revolve around areas where the civil law is simply not up to the task constraining certain wilful and unacceptable behaviour which has serious social consequences.

Discussion paper and submissions

- 12.16.3 In the discussion paper I sought comments upon the general approach to be taken in introducing new offence provisions into the Act as well as seeking comments upon two specific offence provisions I had been considering.
- 12.16.4 Submissions were divided on whether it is appropriate to consider introducing new offence provisions into an Act largely based on civil remedies. However, there was strong support for specific offence provisions where a person intentionally misleads an agency into giving access to information by impersonating the individual concerned or misrepresenting authorisation from that person.

¹⁵ See paragraph 1.6.

¹⁶ See case notes 3734, 6998 and 14824.

“The Group sees the issues as concerning the extent to which the criminal law is the appropriate means of providing incentives to comply with the Act. Where the matter raises questions of the public interest, or where there is a need to constrain truly dishonest or criminal behaviour (eg. knowingly impersonating an individual to make an access request for pecuniary gain) then there is a legitimate involvement of the criminal law.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION G22

Similarly, there was support for creating a specific offence of knowingly destroying information to which a person is entitled to have access in order to deny the person that right. There was also support for including computer crimes such as hacking in the Privacy Act, with a number of submissions preferring such offences to be placed elsewhere such as the Crimes Act.

Impersonating the individual concerned

- 12.16.5 The first new offence that I recommend be created concerns the actions of any person who knowingly makes a request for access to, or correction of, personal information under false pretences. This proposal reflects, in part, the fact that the Privacy Act has obliged agencies in the private sector to open up their files to individuals where previously they may have kept them far more securely closed to outsiders. In such circumstances the agency is put at risk, as is the privacy of the individual concerned, if a person impersonates the individual entitled to have access or misrepresents the position by falsely claiming to have authorisation to have access to information.
- 12.16.6 Presently, the only remedy for the aggrieved individual is to take a complaint against the agency. At best, the individual may obtain redress from the duped agency for disclosure of information or a failure to take reasonable security safeguards, but may well obtain no redress because the security safeguards were, in the circumstances, adequate. Typically there will be no recourse under the Privacy Act against the individual who had deliberately misrepresented the position. In many cases the individual who has used false pretences to obtain the information can take advantage of the domestic affairs exemption in section 56 of the Act if they can show that they collected the information in connection with their personal, family or household affairs.
- 12.16.7 Many businesses feel vulnerable to such deception. Yet there has to be a sensible standard regarding security safeguards to ensure that business and government can operate efficiently. A person who steals an object of value or obtains it by false pretences commits an offence. Access to personal information may sometimes have considerable value but, whether it does or not, the law needs to make plain that obtaining it by deception is not acceptable in any circumstances.
- 12.16.8 This issue is addressed in other jurisdictions. The Australian Privacy Act, for instance, provides that a person must not, by a false pretence, obtain access to an individual's credit information file or credit report in the possession or control of a credit reporting agency. The penalty for breach is a \$30,000 fine¹⁷. The Hong Kong Personal Data (Privacy) Ordinance creates an offence in respect of a person who, in a data access or correction request, supplies information which is false or misleading in a material particular for the purpose of having the data users concerned comply with the request.¹⁸ The offence carries a fine and imprisonment. The Privacy Act 1974 (USA) provides that any person who knowingly or wilfully requests or obtains any record concerning an individual from an agency under false pretences shall be guilty of a misdemeanour carrying a maximum \$5,000 fine.



RECOMMENDATION 148

There should be an offence provision created concerning any person who intentionally misleads an agency by:

- (a) impersonating the individual concerned; or**
(b) misrepresenting the existence or nature of authorisation from the individual concerned;

in order to make the information available to that person or another person or to have the personal information used, altered or destroyed.

¹⁷ Privacy Act 1988 (Australia), section 18T.

¹⁸ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 64(2).

“The Association considers new offence provisions are warranted for individuals deliberately misleading agencies for the procurement of information. The Association is concerned that a significant number of complaints against banks involve inadvertent release of information to third parties, such as former spouses, who have misled the banks in deliberately seeking such information.”

- NZ BANKERS' ASSOCIATION,
SUBMISSION S40

Destroying requested information to deny access

- 12.16.9 A second offence that I recommend relates to the actions of any person who destroys personal information which has been requested by the individual concerned in order to deny that individual the entitlement to have the request determined or reviewed. It is not intended that this offence extend to agency policies which are to destroy documentation, such as job applications, promptly following the awarding of a position to a successful candidate even though such policies may, in part, be motivated by a wish not to have to hold records available for access. Rather, the offence is directed towards circumstances where an individual requests access and the agency, through a pre-existing policy or through the actions of a person within the agency, destroys the records so that a response may be given that the information does not exist.
- 12.16.10 The reason for proposing such an offence is that in essence the civil law response, involving a complaint and a review of the documents, has been deliberately thwarted. While theoretically it is sometimes possible for the matter to be determined in the absence of the information this is usually quite difficult and sometimes impossible. In any case, the access review in such cases is primarily directed towards seeking to establish what the information was and whether it was properly withheld. The proposed offence focuses upon the reprehensible conduct which would deny individuals their entitlements. Such actions should not be permitted notwithstanding that all or part of the information might have been properly withheld.
- 12.16.11 It may be difficult to undertake such prosecutions. However there are often honest employees within agencies who are disturbed at instructions to destroy records in such circumstances who may act as “whistleblowers”. The existence of such an offence will be apparent to privacy officers and people administering the Privacy Act. It will, no doubt, be referred to in staff training. Management in agencies will find it difficult to give instructions to destroy records in such circumstances since their employees will be unwilling to carry them out.
- 12.16.12 A precedent for such an offence is to be found in the privacy statute in Alberta.¹⁹ This provides that a person must not “wilfully destroy any records subject to the Act with the intent to evade a request for access to the records”.

**RECOMMENDATION 149**

There should be an offence created of knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade an access request.

Computer crimes

- 12.16.13 Commentators have suggested for many years now that New Zealand’s criminal laws are inadequate in so far as they relate to “hacking” into computer systems. Seven years ago, the Crimes Consultative Committee noted that:

“Computers are now used very widely in our society, yet the traditional property offences cannot deal adequately with misconduct in respect of computers and the information stored on them. New Zealand has fallen behind the United Kingdom and Australia in not having specific legislation relating to computers”²⁰.

- 12.16.14 New Zealand’s law has continued to fall behind as no computer crimes have been enacted since the Crimes Consultative Committee Report. Meanwhile malicious persons may continue to hack into computer systems to view and

¹⁹ Freedom of Information and Protection of Privacy Act 1994 (Alberta), section 86(1)(e).

²⁰ Report of the Crimes Consultative Committee, *Crimes Bill 1989*, April 1991, pages 74-75.

obtain information to which they are not entitled and, on occasion, to cause mayhem. In a recent overseas example it was reported:

“On 27 March [1998] in the District Court in Sydney, [S] was sentenced to three years imprisonment for offences under the Commonwealth Crimes Act computer misuse provisions. [S] had earlier pleaded guilty to charges of inserting data into a computer and unlawful access to computer data.

“According to reports, [S] had hacked into AUSNet’s computer network two months after he was refused a job with the company. [S] altered the company’s home page and published credit card details of identified individuals.

“The incident is said to have cost the company more than \$2 million in lost clients and contracts, and the widespread publicity had contributed to a general lack of consumer and business confidence in the security of the Internet.”²¹

12.16.15 The Crimes Consultative Committee supported the creation of offence provisions concerning the accessing of a computer for dishonest purposes and damaging or interfering with a computer system. The discussion paper asked whether the Privacy Act should include any computer crimes such as hacking into a computer in order to obtain access to personal information or to manipulate such information. Most of the responses offered support for the creation of computer offence provisions but not all saw the Privacy Act as the appropriate vehicle.²²

12.16.16 Privacy may be enhanced by the existence of appropriate computer-based criminal sanctions but I am not convinced that the Privacy Act is the appropriate vehicle to create such offence provisions. There is information besides personal information which the creation of offences would protect. Hackers have the potential to undermine information security and privacy through their activities and the Privacy Act’s principles and complaints mechanisms alone cannot provide an appropriate response. The main focus of the Act is the obligations on agencies which hold information whereas the focus of computer crimes laws would be the actions of hackers. The existence of offence provisions would provide a deterrent to such activity. I urge the enactment of offences such as those recommended by the Crimes Consultative Committee.

Time for laying information

12.16.17 Section 14 of the Summary Proceedings Act 1957 states:

“Except where some other period of limitation is provided by the Act creating the offence or by any other Act, every information for an offence (other than an offence which may be dealt with summarily under section 6 of this Act) shall be laid within six months from the time when the matter of the information arose.”

12.16.18 Accordingly, a prosecution for any of the offences presently listed in section 127, or those proposed to be created, must be commenced within six months.

²¹ “Setting an example - Internet hacker sentenced”, *4/10 Privacy Law & Policy Reporter*, March 1998, page 200.

²² Of 19 respondents, virtually all were in favour (or appeared to be) of a proposition that the Privacy Act include computer offence provisions in it. 12 submissions explicitly supported the proposition - G1, G2, G4, G6, G8, S13, S21, S36, S42, S45, S46 and S54. Of the remaining 7 submissions all but two supported the creation of an offence provision but opposed the use of the Privacy Act as a vehicle for doing so - G10, G12, G21, G22 and S2. One opposed the proposition that there be such computer crimes (G18) and the other favoured a civil, not criminal, response (G5).

“While WCC believes there needs to be offence provisions for computer crimes such as hacking, it is debatable whether the Privacy Act is the best place. The Crimes Act may be a more logical place as it should apply to all hacking, rather than just for personal information.”

- WELLINGTON CITY COUNCIL,
SUBMISSION G12

On the two occasions over the last few years where I have referred a matter to the Police for prosecution it has been outside the 6 month limitation period and the prosecution could not be brought. One such case concerned a refusal to comply with a lawful requirement of the Commissioner in the course of a complaint. In that instance the requirement was able to be reissued and the matter was thereby resolved. The other concerned an individual who impersonated an investigator from my office which was only discovered outside the limitation period. Clearly the offending might not be revealed within 6 months.

- 12.16.19 In addition, with the present lengthy complaints queue I am concerned that cases of deliberately destroying information or evidence or misleading my investigation may not be uncovered until many months after the event and that the Summary Proceedings Act limitation period may cause difficulties. I recommend that a 12 month limitation period be substituted.



RECOMMENDATION 150

Section 107 should provide that every information for an offence must be laid within 12 months from the time when the matter of the information arose.

12.17 SECTION 128 - Regulations

- 12.17.1 The Governor-General may make regulations in connection with the operation and administration of the Privacy Act. To date, one set of regulations has been made under the Act: the Privacy Regulations 1993. These provide for the service and giving of notices and other documents for the purposes of the Privacy Act and are issued pursuant to section 128(a).
- 12.17.2 The Complaints Review Tribunal Regulations 1996 are also relevant to Privacy Act proceedings although they are not issued under the Act.²³ These prescribe procedural requirements in respect of the hearing of proceedings under sections 82 and 83 of the Privacy Act as well as proceedings under the Human Rights Act 1993 and the Health and Disability Commissioner Act 1994.
- 12.17.3 In addition to the regulation making powers conferred under section 128, the Governor-General may by Order in Council:
- amend the Second Schedule by adding any item to the public register provisions (section 65);
 - amend the information matching rules in the Fourth Schedule in accordance with the recommendations of the Privacy Commissioner (section 107); and
 - until the power expired on 1 July 1997, amend the Fifth Schedule, which relates to law enforcement information, on the advice of the Minister of Justice given after consultation with the Privacy Commissioner (section 113).
- 12.17.4 In other parts of the report I have made certain proposals which might be implemented through the creation of new regulations. These may need explicit new specific regulation-making powers to be inserted into section 128.

12.18 SECTION 129 - Amendments, repeals and revocations

- 12.18.1 Section 129:
- amended the enactments specified in the Sixth Schedule;
 - repealed the enactments specified in the Seventh Schedule; and
 - revoked the orders specified in the Eighth Schedule.
- 12.18.2 The amendments to sections specified in the Sixth Schedule:
- omitted references to the Wanganui Computer Centre Act 1976 and related references to the Wanganui Computer Centre itself;

²³ The 1996 regulations replaced the Complaints Review Tribunal Regulations (No. 2) 1993.

- inserted references to section 105B of the Crimes Act in certain statutes referring to bribery and corruption where these presently refer to section 105A;²⁴
- substituted Privacy Act references for those relating to the Privacy Commissioner Act 1991;
- removed references to the Wanganui Computer Centre Privacy Commissioner as an Officer of Parliament.

12.18.3 The statutes repealed in the Seventh Schedule included:

- the Wanganui Computer Centre Act 1976 (together with subsequent amendments and various references in other statutes);
- the Privacy Commissioner Act 1991 (together with various references to that in other statutes).

12.18.4 The revoked orders in the Eighth Schedule were all made pursuant to the Wanganui Computer Centre Act.

12.18.5 One apparently unforeseen result of the repeal of the Wanganui Computer Centre Act was the diminution of access and correction rights for non-New Zealanders. This is discussed in relation to section 34.²⁵

Repeal of Wanganui Computer Centre Act

12.18.6 One particular consequence of the repeal of the Wanganui Computer Centre Act which has had a deleterious effect on privacy has been the repeal of the offence provision that was contained in section 29(2)(c). That provided:

“Every person commits an offence and is liable on conviction on indictment to imprisonment for a term not exceeding two years who requires any person to obtain under section 14 of this Act, or to produce, for any reason whatsoever, or penalises any person for failing to so obtain or produce, a copy from the computer system of all or a part of the law enforcement information that the person is entitled to receive, or has received, upon an application under section 14 of this Act.”

12.18.7 This provision essentially outlawed what may be referred to as “coerced access requests” or “coerced authorised disclosures” of criminal history information, that is the information concerning existence or absence of convictions, and the details of any conviction.²⁶ It was anticipated that with the repeal of the 1976 Act there would be some administrative changes in obtaining access to criminal history information²⁷ but otherwise things would largely remain the same albeit with “Wanganui” access rights subsumed within principle 6 rights. The extensive list of offences in the Wanganui Computer Centre Act - the one quoted is amongst 10 offences in that section - were not continued as they were seen as generally incompatible with the scheme of the Privacy Act which places the emphasis on civil remedies rather than criminal prosecutions.

²⁴ Section 105B, which was part of the package of reforms made by the select committee which studied the Privacy of Information Bill, is discussed in relation to section 118 at paragraph 12.7.

²⁵ See paragraphs 5.3.1 - 5.3.16 and recommendation 61.

²⁶ A coerced access request would be where, say, a prospective employer insists that an applicant make an access request to an agency and deliver the results to the employer. From the perspective of the law enforcement agency it appears the same as any other access request. The enforced authorised disclosure would have the prospective employer require the applicant to sign a form authorising the law enforcement agency to disclose directly to the employer. This differs from an ordinary access request.

²⁷ Most notably, access requests would not be lodged with the Wanganui Computer Centre Privacy Commissioner but with the relevant law enforcement agency or agencies themselves.

- 12.18.8 Unfortunately, there has been a rapid and undesirable rise in coerced requests and authorised disclosures. Both types of requests were unlawful under the Wanganui Computer Centre Act although those of the first type were difficult to detect. The second are plain enough. Figures supplied by the Department for Courts make it plain that there has been a huge growth in requests for criminal history information including of the second type for which there were none prior to 1 July 1993.
- 12.18.9 The Department for Courts presented statistics showing a significant rise in the number of requests for the release of criminal history information, including a doubling of requests in some months between 1996 and 1997.²⁸ The Department observed that a greater number of employers, particularly those involved in the financial and insurance sectors, are seeking criminal conviction checks. The Department anticipated that the Financial Advisers Disclosure Act 1997 would increase the number of requests, which it estimated as increasing at a rate of 20% per year.
- 12.18.10 The Department had presented the material primarily to explain its difficulties in processing so many access requests and the costs that it believed it had to absorb. However, the position is far more worrying from a privacy perspective. The Department confirmed that *only 25% of requests to the Department for criminal history information come from individuals with the remaining 75% originating from third parties such as insurance companies and prospective employers.*²⁹ I expect that the increasing number of access requests from individuals may also be attributed to third party demands (that is, coerced access requests) since access rights have existed since 1977 and might be expected to increase only modestly if driven solely by the interest of the individuals themselves.
- 12.18.11 This offers a dramatic illustration of the rapid establishment and escalation of coerced access requests and coerced authorised disclosures. It would appear plain that three-quarters of the public releases of criminal history information by the Department would not have been permitted under the 1976 Act. The change has not been positive for privacy and it is worrying that, without some change in the law or administrative practice, the rate of disclosure will likely increase even further. There are a variety of privacy concerns in relation to the coerced release of criminal history information. One particular problem with the present New Zealand arrangements is that the Department for Courts has a practice of releasing a list of all convictions regardless of whether the requester simply wishes to have confirmation of the existence of, or details relating to, a class of convictions or convictions since a certain date. This in itself gives rise to an issue in relation to the disclosure of irrelevant information, the release of which has neither been requested nor authorised.
- 12.18.12 There is not even a cost constraint on prospective employers and insurance companies given that the Department is characterising authorised disclosures as information privacy requests and accordingly providing the information without charge.³⁰ Some private investigators are advertising services which imply they offer an investigation into criminal records but which require the prospective employee to make the access request.
- 12.18.13 It is true that there are interests which compete with privacy in the context of the disclosure of criminal history information. It would be possible to devise alternative schemes, involving vetting or clearance certificates which would provide more satisfactory practices regarding release of information where war-

²⁸ Submission S33.

²⁹ Letter Department for Courts to Office of the Privacy Commissioner, 24 November 1997.

³⁰ Privacy Act, section 35(1), prohibits public sector agencies from making a change for an information privacy request.

ranted in the public interest. My concern in this context is that a dramatic change has resulted which was not preceded by any public debate or clear Parliamentary intention. Instead, I understand that it was anticipated that things would continue much as they have before albeit that the Privacy Commissioner would no longer be the entry point for seeking access to Wanganui Computer information.

12.18.14 I recommend that provision be made to reinstate special controls on individual access rights to criminal history information to ensure that information is only released directly to the individual concerned. Disclosure to third parties, such as insurance companies or prospective employers, should only be permitted where there is both:

- express legislative authorisation; and
- written authorisation from the individual concerned.

12.18.15 Specific authority could be provided in an Act, or regulations, providing for the disclosure to a third party where the objectives of that legislation required. For example, in respect of the Financial Advisers Disclosure Act, mentioned in the departmental submission, there would be a need to:

- identify the relevant convictions (for instance, crimes of dishonesty);
- identify the institutions entitled to have such conviction information (for instance, employers of financial advisers);
- prescribe a form and procedure whereby the individual gives written authorisation to the institution to obtain the relevant details.

12.18.16 As well as having benefits for privacy, this approach would likely smooth implementation of initiatives, such as the screening of financial advisers, and thereby make it more effective. The legislation could also establish fees so that the costs are borne by industry or the Government, as appropriate to the particular proposal, and not publicly subsidised by disguising the process as individuals seeking access to their information under information privacy principle 6. That approach would be consistent with the approach recommended by the International Labour Organisation in the employment context. In its recent commentary to a code of practice on the protection of workers' personal data the ILO states:

“As far as criminal convictions are concerned, collection should again be strictly confined to data clearly relevant to the particular employment. For example, in the case of employment involving child care or work with children, a person previously convicted of child molesting should be obliged to expose the fact. A professional driver could likewise be required to disclose information on previous drunk driving convictions. Data about convictions should be obtained directly from the person concerned so as to ensure that only pertinent information is collected. For the same reason, employers should not be allowed to ask workers to provide a copy of their conviction records.”³¹

12.18.17 There has been concern in Britain at the issue of coerced access requests and a provision has been included in the new Data Protection Bill to prohibit the practice. The clause provides in part:

“Prohibition of requirement as to production of certain records

- (1) a person must not, in connection with:
- (a) the recruitment of another person as an employee;

“The Department has some indication that some private investigators and insurance companies are requesting information on criminal convictions with a falsified authorisation signature or a photocopy of that signature from another document.”

- DEPARTMENT FOR COURTS,
SUBMISSION S33

³¹ International Labour Office, *Protection of Workers' Personal Data*, an ILO code of practice 1997, pages 31-32.

- (b) the continued employment of another person; or
 - (c) any contract for the provision of services to whom by another person;
- require that other person or a third party to supply him with a relevant record or to produce a relevant record to him.
- (2) A person concerned with the provision (for payment or not) of goods, facilities or services to the public or a section of a public must not, as a condition of providing or offering to provide any goods, facilities or services to another person, require that other person or a third party to supply him with a relevant record or to produce a relevant record to him.
 - (3) Subsections (1) and (2) do not apply to a person who shows:
 - (a) that the imposition of the requirement was required or authorised by or under any enactment, by any rule of law or by the order of a court; or
 - (b) or that in particular requirements that the imposition of the requirement was justified as being in the public interest.
 - (4) Having regard to the provisions of Part V of the Police Act 1997 (Certificates of Criminal Records etc), the imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as being justified as being in the public interest on the ground that it would assist in the prevention or detection of crime.
 - (5) A person who contravenes subsection (1) or (2) is guilty of an offence.”³²

A table is set out which lists certain criminal history information, as “relevant records” notably convictions and cautions.



RECOMMENDATION 151

A provision should be included to prohibit employers, prospective employers, and providers of services, requiring individuals to exercise their access rights to obtain criminal history information as a condition of obtaining employment, continuing employment, or obtaining services.

Coerced access requests - medical records

12.18.18 The problem of coerced access requests, and coerced authorised disclosure, has been manifested primarily in relation to criminal history information. This is the area in which the operation of the Privacy Act has, in a sense, created the problem through the repeal of the Wanganui Computer Centre Act 1976. However, it is not the sole area in which the issue arises. In societies of our type there has been growing problem of employers and insurance companies insisting upon individuals exercising access rights to their health records and delivering a copy to the employer or the insurer. This differs from the practice of employers or insurance companies requiring an individual to undergo a medical examination by the employer’s or insurer’s medical practitioner - a practice which is not of concern in this context. The new UK Bill has tackled this issue with a clause which provides:

“Avoidance of certain contractual terms relating to health records

- (1) Any term or condition of a contract is void in so far as it is purports to require an individual to supply any other

³² Data Protection Bill [HL] (UK), 4 June 1998 version, clause 56(1)-(5).

- person with a record to which this section applies, or with a copy of such a record or a part of such a record.
- (2) This section applies to any record which:
- (a) has been or is to be obtained by a data subject in the exercise of the right conferred by section 7; and
 - (b) consists of the information contained in any health record as defined by section 68(2).³³

Clause 68 defines “health record” to mean any record which:

- (a) consists of information relating to the physical or mental health or condition of an individual; and
- (b) has been made by or on behalf of a health professional in connection with the care of that individual

12.18.19 The problem of coerced access, and coerced authorised disclosure, will continue to grow especially as insurance enters further aspects of our national life. Already, over the last several years, a greater interest by employers has been shown in the health records of their employees as a result of the experience rating system adopted since 1992 in the accident compensation legislation. It is appropriate to have a similar provision to the UK clause in our own Act or at least allow for the same effect to be achieved in a code of practice.



RECOMMENDATION 152

Provision should be made to constrain contractual requirements that oblige individuals to supply copies of health records.

12.19 SECTION 130 - Final report of Wanganui Computer Centre Privacy Commissioner

12.19.1 Section 130 provided for the final report of the Wanganui Computer Centre Privacy Commissioner. The provision was necessary because the final report was submitted after the repeal of the Wanganui Computer Centre Act 1976 pursuant to which previous annual reports were filed. Since the Wanganui Computer Centre Privacy Commissioner was no longer an Officer of Parliament there was no jurisdiction for a report to be presented directly to Parliament. Instead, provision was made for the final report to be submitted to the Minister of State Services who subsequently laid the report before the House of Representatives.

12.19.2 The report was made by P L Molineaux in 1993 and the provision is now spent.³⁴

12.20 SECTION 131 - Privacy Commissioner to complete work in progress of Wanganui Computer Centre Privacy Commissioner

12.20.1 This provision empowered me as Privacy Commissioner, to complete the work in progress of the Wanganui Computer Centre Privacy Commissioner. I reported on the work undertaken in that capacity in my 1993/94 and 1994/95 annual reports.³⁵

12.20.2 At the start of the 1993/94 year there were nine complaints still under investigation. At the beginning of the 1994/95 year seven remained under investigation but all were concluded by the end of that year.

12.20.3 With the repeal of the Wanganui Computer Centre Act 1976 it was also neces-

³³ Data Protection Bill [HL] (UK), 4 June 1998 version, clause 57.

³⁴ See *Final Report of the Wanganui Computer Centre Privacy Commissioner for the year ended 30 June 1993*, AJHR, A4.

³⁵ See *Report of the Privacy Commissioner for the year ended 30 June 1994*, page 12, and *Report of the Privacy Commissioner for the year ended 30 June 1995*, page 13.

sary for me to review the status of the files of the former Wanganui Computer Centre Privacy Commissioner. The review was completed during the 1993/94 year in consultation with the Chief Archivist. Some files were transferred for archiving and some were destroyed.

12.21 SECTION 132 - Savings

12.21.1 Section 132 provides that, for the avoidance of doubt, and without limiting the Acts Interpretation Act, the repeal of the Wanganui Computer Centre Act shall not affect:

- the continuing existence of the Wanganui Computer Centre;
- the computer system established in connection with that computer centre;
- or
- any agreements or arrangements entered into by the Minister of State Services pursuant to section 3A of that Act.

12.21.2 I expect that that provision was included out of an abundance of caution and was actually entirely unnecessary. It is interesting to note that the “continuing existence” of the Wanganui Computer Centre is now mainly in the collective national psyche given that the computer systems formerly operated out of Wanganui are now located somewhere in Auckland. Furthermore, all law enforcement agencies are now in the process of “migrating” away from the Law Enforcement System or are planning to do so by the year 2000. Out of an abundance of caution section 132 provides that the repeal of the Wanganui Computer Centre Act does not affect the continuing existence of the Wanganui Computer Centre - but does its physical removal? Does the fact that law enforcement agencies are ceasing to use it affect its continuing existence? When exactly *does* a computer system cease to exist?

12.21.3 I take the view that section 132 was probably never needed. If it was, its need has now passed. As a tidying up exercise to remove “clutter” from the Act I would like to see section 132 repealed. It may also be undesirable to have two sections of the Act (sections 7 and 132) carrying the same marginal note “savings”.



RECOMMENDATION 153

Section 132 should be repealed.

12.22 SECTION 133 - Transitional provisions

12.22.1 The transitional provision contained in section 133 was necessary because of my appointment under the Privacy Commissioner Act 1991. This provision converted that into a continuing appointment under the current Act.