

Chapter 5

Exclusions and exemptions

- 5.1 A number of provisions in the Privacy Act limit the application of the privacy principles in various ways, or exempt certain entities or types of information from the application of the privacy principles altogether. This chapter examines some key provisions in the Act that create exclusions and exemptions from the privacy principles. A number of other types of exclusions, exemptions and exceptions are discussed in other chapters of the issues paper.

BACKGROUND

- 5.2 Privacy is not an absolute right, and other rights or interests will sometimes take precedence over it. For example, privacy interests may be outweighed by such public interests as national security, health and safety, or freedom of information. By providing for exclusions, exemptions and exceptions, information privacy laws recognise the need to balance privacy against such other interests.
- 5.3 International human rights and privacy instruments recognise that the right to privacy can legitimately be limited for various reasons. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to “arbitrary or unlawful” interference with privacy. This wording implies that interferences with privacy will sometimes be allowed, providing they are lawful and are not arbitrary. The Human Rights Committee, the body with official responsibility for monitoring implementation of the ICCPR, has recognised in a General Comment on article 17 that “As all persons live in society, the protection of privacy is necessarily relative.” However, any interferences with the right to privacy must be authorised and specified by law, must comply with the aims and objectives of the ICCPR, and must be reasonable in the circumstances.³⁶⁰ The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data also contemplate that states may create

360 Human Rights Committee “General Comment 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17)” (8 April 1988). See also European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8(2), which permits only such interference with the right to privacy as is “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

exceptions to the principles set out in the Guidelines, but state that such exceptions should be as few as possible and should be made known to the public.³⁶¹

- 5.4 Blair Stewart of the Office of the Privacy Commissioner notes that drafting and locating exceptions to privacy laws “is not a technical matter of little importance”, since such exceptions define the extent of the privacy principles. Getting exceptions right, he continues, can enhance:³⁶²
- the workability of a law;
 - the clear understanding of legal obligations;
 - the appropriate workload of a small Privacy Commissioner’s office;
 - the timeliness of sorting out business compliance difficulties;
 - the flexibility of the law; and
 - the appropriate response to lobbying for special favours.
- 5.5 Distinctions can be drawn between the following ways in which the Act provides that the privacy principles may not apply, or that their application may be modified, in certain cases:³⁶³
- **Exclusions** refer to entities or types of information that are not covered by the privacy principles at all. For example, the privacy principles do not apply at all to the news media in the course of their news activities (with a limited exception for Radio New Zealand and Television New Zealand).
 - **Exemptions** provide that particular types of agency or information, although not excluded altogether from the scheme of the Act, do not have to comply with certain privacy principles. For example, the intelligence organisations are required to comply only with principles 6, 7 and 12. Alternatively, the application of some privacy principles to certain agencies could be modified so that the principles are easier to comply with.
 - **Exceptions** are general in application, and allow for particular privacy principles not to be complied with on certain grounds. That is, they place limits on the scope of the principles themselves. There are detailed exceptions in several of the principles. For example, there are exceptions to principles 2, 10 and 11 that allow for collection, use or disclosure of personal information that is publicly available.
- 5.6 In this chapter we discuss entities that are excluded from the coverage of the privacy principles by being excluded from the definition of “agency”, and certain exemptions provided for in Part 6 of the Act. Other exclusions, exemptions and exceptions are discussed elsewhere in the issues paper:
- Some information is excluded from the coverage of the Act by the definitions of “individual” and “personal information”, as discussed in chapter 3. In particular, the Act does not apply to information about deceased persons or legal persons.

361 Organisation for Economic Development and Cooperation “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (1980), para 4. See also paras 46–47 of the Explanatory Memorandum to the Guidelines.

362 Blair Stewart “The New Privacy Laws: Exemptions and Exceptions to Privacy” (paper presented to The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

363 See Blair Stewart “The New Privacy Laws: Exemptions and Exceptions to Privacy” (paper presented to The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

- Chapter 4 discusses exceptions contained in the principles themselves, as well as the “good reasons for refusing access” (which are effectively exceptions to principle 6) set out in Part 4 of the Act.
- Codes of practice, discussed in chapter 7, can modify the application of the principles by prescribing standards that are more or less stringent than those that would normally apply, or by exempting any action from any privacy principle. Codes that provide for less stringent standards are effectively a type of exemption.
- The Act provides for authorised information matching programmes in the public sector, as discussed in chapter 9. Such programmes are effectively exempted from the application of the privacy principles, and are instead subject to a set of information matching rules set out in Schedule 4 to the Act.
- As discussed in chapter 11, other laws can override the Privacy Act, effectively creating exceptions to the application of the privacy principles.
- Law enforcement exceptions are discussed in chapter 12.

EXCLUSIONS FROM THE DEFINITION OF “AGENCY”

- 5.7 Section 2(1) of the Privacy Act provides that an agency means “any person or body of persons, whether corporate or incorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department”. However, the definition goes on to state that certain entities or types of entity are excluded from the definition of “agency”. The definition of “agency” does not include:
- (i) The Sovereign; or
 - (ii) The Governor-General or the Administrator of the Government; or
 - (iii) The House of Representatives; or
 - (iv) A member of Parliament in his or her official capacity; or
 - (v) The Parliamentary Service Commission; or
 - (vi) The Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; or
 - (vii) In relation to its judicial functions, a court; or
 - (viii) In relation to its judicial functions, a tribunal; or
 - (ix) An Ombudsman; or
 - (x) A Royal Commission; or
 - (xi) A commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; or
 - (xii) A commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; or
 - (xiii) In relation to its news activities, any news medium.
- 5.8 The effect of these exclusions is that the listed entities are not required to comply with the privacy principles, since the principles refer to information that is collected, held, used or disclosed by an agency, or in the case of principle 12, to unique identifiers that are assigned by an agency. Entities that are excluded from the definition of “agency” therefore cannot breach the privacy principles, which in turn means that they cannot be the subject of complaints about breaches of the principles. It is important to note, however, that there is nothing to prevent

the Privacy Commissioner from commenting or reporting on the actions of entities that are excluded from the definition of “agency”, pursuant to her general functions relating to “the privacy of the individual” under section 13 of the Act.

- 5.9 At present, the entities excluded from the definition of “agency” are thereby exempted from all of the privacy principles, although in some cases the exemptions are limited in certain respects (for example, members of Parliament are only exempted in their official capacities). In considering options for reform, it should be borne in mind that these entities could be made subject to some but not all of the principles, if it is considered desirable that certain privacy principles should apply to them.
- 5.10 We are not aware of any issues that require consideration with regard to the exclusions of the Sovereign, Governor-General or Administrator, courts, tribunals, or Royal Commissions or other public inquiries. In relation to courts and tribunals, we note that their exclusion applies only to the exercise of their judicial functions. In our *Access to Court Records* report, we considered whether this exclusion extended to court records even after a matter is finally determined and all appeal rights have been exhausted. We concluded that it did, and that the Privacy Act does not apply to court records.³⁶⁴ Privacy is, however, recognised in court rules as a matter to be taken into account when considering applications for access to court documents, files or records.³⁶⁵ With regard to the various forms of public inquiry, the Law Commission’s report on *A New Inquiries Act* recommended that privacy should be one of the grounds for restricting public access to inquiries, and this is reflected in the Inquiries Bill currently before Parliament.³⁶⁶

House of Representatives and Members of Parliament

- 5.11 The House of Representatives is excluded from the definition of “agency”, and MPs are excluded in their “official capacity”. The then Privacy Commissioner discussed these exceptions in *Necessary and Desirable*. With regard to the House of Representatives, the Commissioner noted that privacy is protected to some degree by Standing Orders and other rules and practices of the House. He concluded that if any of the privacy principles (particularly the access principle) were to be applied to the House, this should be done by Standing Orders rather than by statute, and that it would be best for the initiative to come from Parliament itself. He recommended that the matter be considered by an appropriate committee of Parliament.³⁶⁷
- 5.12 With regard to MPs, the Commissioner noted that the exclusion of “a member of Parliament in his or her official capacity” goes beyond the exemption that would apply as an incidence of Parliamentary privilege. For example, constituency work would fall within the category of activity carried out in the Member’s official capacity. The Commissioner suggested that there would probably be few

364 New Zealand Law Commission *Access to Court Records* (NZLC R93, Wellington, 2006) 55–56.

365 Criminal Proceedings (Access to Court Documents) Rules 2009, r 16(c); Judicature Act 1908, sch 2 (High Court Rules), r 3.16(b); District Court Rules 2009, r 3.22(b).

366 New Zealand Law Commission *A New Inquiries Act* (NZLC R102, Wellington, 2008) 94–95; Inquiries Bill 2008, no 283-1, cl 15(2)(d).

367 *Necessary and Desirable* 36–37, rec 5.

problems in applying some principles, such as principles 4 and 5, to MPs, while others (such as the disclosure principle) would be much more controversial. He raised a particular concern about what happens to personal information in MPs' constituency files when a Member loses office. Again, the Commissioner recommended that the matter be considered by an appropriate committee of Parliament.³⁶⁸

- 5.13 Our provisional view is that these matters should be considered by a committee of Parliament, as recommended by the Privacy Commissioner.

Q61 We propose that the application of the privacy principles (not necessarily by way of the Privacy Act itself) to the House of Representatives and to MPs should be considered by a committee of Parliament. Do you agree?

Parliamentary Service Commission and Parliamentary Service

- 5.14 The Parliamentary Service Commission is entirely excluded from the definition of “agency”. The Parliamentary Service is excluded “except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee”. The Office of the Clerk is covered by the Privacy Act.
- 5.15 In *Necessary and Desirable*, the Privacy Commissioner noted that the then General Manager of the Parliamentary Service could see no reason why the Parliamentary Service, in fulfilling its administrative functions, should not be fully subject to the Act, providing that this could be accomplished without impinging on the exemption for MPs in their official capacities. The Commissioner recommended that either the partial exemption of the Parliamentary Service should be further restricted or the Service should be made fully subject to the Privacy Act, so long as the General Manager's caveat could be accommodated. The Privacy Commissioner also recommended that the exemption for the Parliamentary Service Commission be reviewed to see whether it could be replaced with a partial exemption.³⁶⁹
- 5.16 The Commissioner subsequently considered these exemptions further in a report on the Parliamentary Service Bill, and his recommendations in that report were also included in a supplement to *Necessary and Desirable*. In his report on the Bill, the Commissioner commented that:³⁷⁰

The two exceptions to the Privacy Act primarily reflect a desire to place certain information off limits to access requests. This approach largely continues the thinking which had previously led to complete exemption of the Official Information Act. One of the most important reasons for the exemptions is the fact that members of Parliament themselves have never been subject to the Official Information Act, and are exempted in their official capacities from the Privacy Act, and it would therefore

368 *Necessary and Desirable* 37–39, rec 6.

369 *Necessary and Desirable* 39–40, recs 7 and 8.

370 Bruce Slane, Privacy Commissioner *Report to the Minister of Justice in relation to the Parliamentary Service Bill* (2 November 1999).

be problematic to make parliamentary service bodies subject if that meant indirect access to documents prepared or held by members of Parliament. This is especially a consideration for the Parliamentary Service Commission which is made up of MPs. It is also an issue for the Parliamentary Service given that it employs the staff who actually work in MPs' offices.

Accordingly, it appears to me that the main desire for an exemption for the two parliamentary service bodies relates to the rights of access contained in principle 6 rather than any concern about the remaining 11 information privacy principles.

- 5.17 The Commissioner therefore recommended that both the Parliamentary Service Commission and the Parliamentary Service be made subject to all of the privacy principles except for principle 6. In addition, he recommended that the principle 6 right of access should apply to the Parliamentary Service in respect of its employees (as it does already) and that this should also be extended to cover prospective employees and contractors.³⁷¹ The Government Administration Committee's response to these recommendations in its report on the Parliamentary Service Bill was inconclusive, but the Committee stated that these issues would best be addressed when a general amendment to the Privacy Act is being considered.³⁷²
- 5.18 We believe that these matters are best considered together with the issues concerning the House of Representatives and MPs. We therefore propose that the Privacy Commissioner's recommendations with regard to the Parliamentary Service and the Parliamentary Service Commission should be considered by the same committee of Parliament that considers the application of the privacy principles to the House and MPs.

Q62 We propose that the issue of extending the privacy principles to the parliamentary service bodies should be reviewed by a committee of Parliament at the same time as that committee considers the application of the principles to the House of Representatives and MPs. Do you agree?

Ombudsmen

- 5.19 The Ombudsmen are excluded entirely from the definition of "agency". In *Necessary and Desirable*, the former Privacy Commissioner argued that there were three features of the Ombudsmen which might seem to warrant their exemption from the Privacy Act:
- their status as the review authority for Official Information Act (OIA) complaints;
 - their status as officers of Parliament; and
 - their status as a complaints body.

³⁷¹ Bruce Slane, *Privacy Commissioner Report to the Minister of Justice in relation to the Parliamentary Service Bill* (2 November 1999); *1st supplement to Necessary and Desirable*, recs 7A and 8A.

³⁷² Government Administration Committee *Report on the Parliamentary Service Bill* (2000) 10.

- 5.20 With regard to the first point, the Commissioner considered that, at most, the Ombudsmen’s role as the review authority for OIA complaints might warrant a partial exemption from principle 6. This is already covered, the Commissioner argued, by section 55(d) of the Privacy Act, which provides that principles 6 and 7 do not apply to information in correspondence and communication between the Ombudsmen and any other agency in relation to investigations under the Ombudsmen Act, the OIA or the Local Government Official Information and Meetings Act.
- 5.21 On the second point, the Commissioner noted that the Auditor-General and the Parliamentary Commissioner for the Environment are not exempted from the Privacy Act, and that the Ombudsmen are subject to the Human Rights Act but not to the Privacy Act. The Commissioner did not consider that the Ombudsmen’s status as officers of Parliament should place them outside the application of the privacy principles.
- 5.22 Regarding the third point, the Commissioner saw nothing inappropriate about a complaints body being subject to complaints to another complaints body, noting that, for example, the Privacy Commissioner can be the subject of complaints to the Ombudsmen and the Human Rights Commission. Making an institution subject to a complaints mechanism “does not undermine public confidence in it but rather strengthens it”.
- 5.23 The Commissioner therefore recommended that the Ombudsmen should be made subject to the privacy principles. He noted that some overseas privacy laws expressly apply to ombudsmen.³⁷³ We currently support the Commissioner’s recommendation.

Q63 We propose that the Ombudsmen should be made subject to the privacy principles. Do you agree?

News media

- 5.24 “Agency” is defined as not including “in relation to its news activities, any news medium.” “News activity” is defined to mean:

the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:

the dissemination, to the public or any section of the public, of any article or programme of or concerning –

- (i) news:
- (ii) observations on news:
- (iii) current affairs.

“News medium” is defined to mean “any agency whose business, or part of whose business, consists of a news activity; but, in relation to principles 6 and 7, does not include Radio New Zealand Limited or Television New Zealand Limited.”

³⁷³ *Necessary and Desirable* 42–43, rec 10.

- 5.25 We believe the exclusion is justified. The free flow of information in the media is a crucial element of a free and democratic society. It is supported by section 14 of the New Zealand Bill of Rights Act 1990.³⁷⁴ To require the media to comply with the privacy principles would be to impose an unreasonable limit on that freedom. It would not merely impede the media, but virtually hamstring it, to have to comply with, for example, principle 2 (personal information to be collected directly from the individual) and principle 11 (personal information not to be disclosed).
- 5.26 The Privacy Act is not unusual in granting the media or journalists an exemption from its provisions. So, for example, do the Fair Trading Act 1986,³⁷⁵ the Financial Advisers Act 2008³⁷⁶ and the various statutes regulating attendance at court proceedings.³⁷⁷ Similar exceptions for media and journalism also exist in overseas privacy statutes.³⁷⁸
- 5.27 It is not as though the media are exempt from privacy laws and rules altogether: broadcasters are subject to the jurisdiction of the Broadcasting Standards Authority, and the print media to that of the Press Council. Those bodies can fashion principles appropriate to the media's special function. In addition, the media are potentially subject to the range of tortious and criminal liability that we have noted in Stage 3 of our Review. Moreover, the media do not fall outside the Privacy Commissioner's function of inquiring into, making statements about, and reporting on, matters affecting privacy.

"News activity"

- 5.28 While we believe that the news media exclusion should remain, there are questions about the way it is defined, and its confinement to the news media "in relation to its news activities." There has been debate about the meaning of "news activity". There are currently three possible interpretations:³⁷⁹
- That the media organisation is protected so long as it was acting in its capacity as a mass communicator, as opposed, for example, to its capacity as an employer (the "capacity" test).
 - That the organisation is protected only so long as it is publishing news, or news-related material, which contains an element of public interest (the "public interest" test).
 - That the organisation is protected only so long as it is publishing material within the genre of news and current affairs as opposed, say, to the genre of entertainment (the "genre" test).

374 Section 14 of the New Zealand Bill of Rights Act 1990 provides for the "right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind in any form."

375 Fair Trading Act 1986, s 15.

376 Financial Advisers Act 2008, s 12(a).

377 For example, Criminal Justice Act 1985, s 138(3).

378 Privacy Act 1988 (Cth), s 7B(4); Data Protection Act 1998 (UK), s 32; Personal Information Protection and Electronic Documents Act SC 2000 c 5 (Canada), ss 4(2)(c), 7(1)(c).

379 See Elizabeth Paton-Simpson "The News Activity Exemption in the Privacy Act 1993" (2000) 6 NZBLQ 269.

- 5.29 Depending on which interpretation one favours, there could be an argument that, for example, a television reality show, or a humorous column in a newspaper, might fall outside the exemption. It is perhaps surprising that in the 16 years since the Act came into force there have been very few disputed instances. In those cases in which the definition of “news activity” has been at issue, the Privacy Commissioner (and the Tribunal) have taken a view quite generous to the media, holding for example that the *National Business Review*’s “Rich List”³⁸⁰ and the television programme “Target”³⁸¹ are covered by the exemption. In such cases, of course, a failed complainant is not deprived of recourse: he or she can still complain to the Broadcasting Standards Authority, or, in the case of the print media, to the Press Council, although it is true that in the latter case there can be no substantive remedy such as damages.
- 5.30 The question is whether it would be possible to define “news activity” with any greater precision. Given the increasingly unclear line between news and entertainment, and the uncertain boundaries of even the term “news” itself, that would be a very difficult undertaking. Any formulation would still leave much to judgment in marginal cases. Our preferred position, therefore, is to leave the present wording as it is, and allow the Privacy Commissioner (and in appropriate cases the Tribunal) to make judgment calls on a case-by-case basis.

“News medium”

- 5.31 There is a further difficulty in determining the boundaries of the term “news medium”. That is the difficulty of deciding how far it now extends beyond traditional broadcasters and print media to the array of alternative media: blogs and other websites, for instance. The problem manifests itself when one considers the avenues of complaint open to an individual whose privacy is infringed by publication of private information. If publication takes place in the print media, a complaint can be made to the Press Council. If it is in a broadcast, as that term is defined in the Broadcasting Act 1989,³⁸² the Broadcasting Standards Authority has jurisdiction over the matter. But many manifestations of the new media fall outside the sphere of both of these bodies. The question is whether complaints against these new media for breach of principle 11 can be investigated by the Privacy Commissioner. It will not be possible for the Commissioner to investigate if the websites or other media in question fall within the “news media” exception in section 2 of the Privacy Act. Most online publications (other than those associated with a print publication such as a newspaper or magazine, or with a broadcaster) would probably not fall within the news media exception because they are not in “business”.³⁸³ But there might be a few regular blogs or other online publications which, arguably, could be regarded as being “news media” within the definition in section 2. If that is so, there may be a few manifestations of the new electronic media which are not subject to any of the existing complaints jurisdictions – Press Council, Broadcasting Standards Authority, or Privacy Commissioner.

380 *Talley Family v National Business Review* (1997) 4 HRNZ 72.

381 *TV Technician Complains About Being Covertly Filmed for a TV Programme* [2003] NZ PrivCmr 24 – Case Note 38197.

382 See definitions of “broadcaster” and “broadcasting” in Broadcasting Act 1989, s 2(1).

383 There may be some argument about what “business” means in this context, however.

5.32 We wonder whether the definition of “news medium” should be amended to confine it in some way. On the one hand, this would avoid the possibilities of some publications, few though they might be, slipping through the net altogether. On the other, it might be argued that the privacy principles are simply not appropriate to any branch of the media. If it is considered desirable to restrict the meaning of “news medium”, one option would be to confine it to print and broadcast media. However, this would mean that online versions of newspapers or broadcasts would be subject to complaints to the Privacy Commissioner unless a way could be found of excluding them. It would clearly be absurd if a person could not complain to the Privacy Commissioner about an article that appears in print, but could complain about the same article when it appears on a newspaper’s website. An alternative option would be to provide in the Act that a news medium can only benefit from the Privacy Act exclusion if it is subject to a code of ethics and to a complaints procedure administered by an appropriate body (the Press Council, the Broadcasting Standards Authority, or any other relevant complaints body that might be established in future). The media exception in the Privacy Act 1988 (Cth) includes a provision somewhat along these lines.³⁸⁴ We seek views on this matter.

Radio New Zealand and Television New Zealand

5.33 We have concerns about one further matter relating to the definition of “news medium”. That is the subjection of Radio New Zealand Limited (RNZ) and Television New Zealand Limited (TVNZ) to principles 6 (access to personal information) and 7 (correction of personal information). Before the Privacy Act was passed, the OIA contained provisions enabling persons to access personal information about them held by agencies subject to that Act. Those access provisions, so far as they related to individuals, were removed to the Privacy Act in 1993. It was obviously felt that, as state broadcasters also subject to the OIA, RNZ and TVNZ were in a different position from other media. We wonder whether that distinction is justified. It is not just that the present provisions give private broadcasters an advantage over the state broadcasters in a very competitive market; subjection to the OIA can have that effect in other contexts too. It is rather that a requirement to allow access to, and correction of, personal information can have an effect – at the very least a delaying effect – on the dissemination of news. It might lead to an application for an injunction,³⁸⁵ for example, or to lengthy stalling debate over whether information held is completely accurate. This might be regarded as an unjustified limitation on freedom of information whether the broadcaster be state or private. We wonder therefore whether the limiting reference to RNZ and TVNZ should be removed from the definition of “news medium” in section 2.³⁸⁶ This would, of course, still preserve the right to access and correct information, such for example as employment information, which falls outside the “news activity” exemption. We acknowledge

384 Privacy Act 1988 (Cth), s 7B(4)(b).

385 Bearing in mind that access rights under principle 6 can be directly enforced in the courts where information held by a public sector agency is concerned: Privacy Act 1993, s 11(1). RNZ and TVNZ are public sector agencies in terms of the Act: Privacy Act 1993, s 2(1), definitions of “public sector agency” and “organisation”; Official Information Act 1982, sch 1.

386 This would also require a corresponding deletion of section 29(1)(g), which allows RNZ and TVNZ to withhold requested information if disclosure would be likely to reveal a journalist’s source.

that an amendment of the kind we suggest would still leave differences between TVNZ and RNZ and the other media, because the state broadcasters would remain subject to the OIA with regard to information held by them.

Q64 We propose that the exclusion of the news media in relation to their news activities should remain in the Privacy Act. Do you agree?

Q65 We propose that the definition of “news activity” should remain as it is. Do you agree?

Q66 Do you think the definition of “news medium” should be amended to confine it to the print and broadcast media? Alternatively, should it be confined to news media that are subject to a code of ethics and complaints procedure?

Q67 We propose that the limiting reference to Radio New Zealand and Television New Zealand should be removed from the definition of “news medium”. Do you agree?

Q68 Are any other changes needed to the exclusions from the definition of “agency”?

SPECIFIC EXEMPTIONS IN PART 6 OF THE ACT

- 5.34 Part 6 of the Act provides for codes of practice (discussed in chapter 7), and for certain other types of specific exemption. Sections 54, 56 and 57 are discussed below. We are not aware of any issues in relation to section 55, which excludes certain types of information from the coverage of principles 6 and 7.

Q69 Are any changes needed to section 55?

Section 54 – authorisation by the Privacy Commissioner

- 5.35 Section 54 provides that the Privacy Commissioner may authorise an agency to collect, use or disclose information where this would otherwise breach principles 2, 10 or 11, if the Commissioner is satisfied that, “in the special circumstances of the case”:

- the public interest outweighs any interference with the privacy of an individual that could result; or
- there is a “clear benefit to the individual concerned” that outweighs any interference with the privacy of the individual that could result.

The Commissioner may impose such conditions as he or she sees fit on such an authorisation. The Commissioner shall not grant an authorisation under section 54 if the person concerned has refused to authorise the collection, use or disclosure of his or her information for the relevant purpose.

- 5.36 The Commissioner has issued a Guidance Note to applicants seeking exemptions under section 54. The Commissioner’s Annual Report includes a report on section 54 applications.³⁸⁷ It seems that there are a few applications each year, but that many are not granted. A common reason for declining applications seems to be that the Commissioner considers that the exemption applied for is unnecessary, because the agency’s objective can be achieved without breaching the privacy principles.
- 5.37 The reference to “the special circumstances of the case” would seem to mean that section 54 is not intended to allow for the granting of ongoing or generic exemptions. This is reinforced by the Commissioner’s Guidance Note, which states:³⁸⁸

Section 54 seems primarily designed for “one-off” situations. If the circumstances giving rise to an application are likely to arise again and again, or are a routine part of an agency’s activities, it is likely that an exemption will be inappropriate. Consideration should instead be given to seeking a code of practice.

Should section 54 apply to other principles?

- 5.38 It is not clear why section 54 applies only to principles 2, 10 and 11. There may be instances in which exceptions to some other principles could be granted on the same basis. It would probably not be appropriate to allow exemptions to be granted in the case of principle 1, which is fundamental to the whole operation of the Act. It is also hard to see why exemptions should ever be allowed for principles 4, 5 and 8. In the *Necessary and Desirable* review, the Privacy Commissioner asked whether the Commissioner’s power to grant exemptions under section 54 should be extended to principles 9 and 12, and finally recommended that the power be extended to principle 9 only.³⁸⁹ We agree that the Commissioner should be able to grant exemptions from principle 9 under section 54.

Q70 We propose that section 54 should be amended to allow the Privacy Commissioner to grant exemptions from principle 9. Do you agree? Should the Commissioner be allowed to grant exemptions under section 54 from any other principles?

Should section 54 be used for ongoing exemptions?

- 5.39 As noted above, OPC considers that section 54 is intended for “one-off” exemptions only. This seems consistent with the wording of the section, particularly the reference to “the special circumstances of the case”. However, it has been suggested to the Law Commission that it should be possible to use section 54 to authorise ongoing collection, use or disclosure, rather than one-off exemptions only.

³⁸⁷ See for example Office of the Privacy Commissioner *Annual Report 2009* (Wellington, June 2009) 34.

³⁸⁸ Office of the Privacy Commissioner “Guidance Note to Applicants Seeking Exemption Under Section 54 of the Privacy Act” (1997) para 3.4.

³⁸⁹ Office of the Privacy Commissioner *Review of the Privacy Act 1993: Discussion Paper No 4: Codes of Practice and Exemptions* (Wellington, 1997) 7–8; *Necessary and Desirable* 219–220, rec 79.

- 5.40 Giving the Privacy Commissioner the power to authorise ongoing exemptions in some cases could be seen as a halfway house between one-off exemptions and the much more involved process of developing and approving a code of practice. It might be useful where a particular issue comes up again and again but is perhaps too specific to warrant the creation of a code.
- 5.41 However, the following cautionary points need to be considered in relation to the suggestion that the Privacy Commissioner could authorise ongoing exemptions under section 54:
- At present there is no evidence of a real problem. There is already quite a lot of flexibility in the privacy principles, and the experience with the existing provisions of section 54 suggests that many applications for ongoing exemptions would be turned down by the Privacy Commissioner on the grounds that what the agency seeks to do is already allowed under the Act.
 - Giving the Commissioner the power to authorise ongoing exemptions would mean giving him or her significant powers to modify the terms of the Act. This is already true of the codes of practice provisions, but these include procedural safeguards relating to consultation and notification. Moreover, we propose in chapter 7 that codes of practice should be approved by Cabinet. Similar safeguards would surely need to be put in place for ongoing exemptions under section 54, in which case it is hard to see how they would differ from codes of practice.
 - It is reasonably easy to see how ongoing exemptions could be justified on public interest grounds (section 54(1)(a)). Exemptions involving “a clear benefit to the individual concerned” (section 54(1)(b)) are a different matter, however. Subsection (1)(b) is more obviously suited to one-off applications relating to specific situations than to ongoing exemptions. It is likely to be difficult to assess the benefit to the individual where ongoing collection, use or disclosure is concerned. The same is probably true with regard to the provision in section 54(3) that an exemption shall not be authorised by the Commissioner where the individual concerned has refused to authorise the collection, use or disclosure. This provision seems to contemplate a one-off opportunity to refuse consent, and might be difficult to apply to an ongoing exemption.
- 5.42 For the reasons given in the above bullet points, we believe that the Privacy Commissioner should not be empowered to authorise ongoing exemptions under section 54.

Q71 We propose that section 54 should continue to be limited to one-off exemptions only. Do you agree?

Q72 Are any other changes needed to section 54?

Section 56 – personal, family or household affairs

5.43 Section 56 is deceptively short and simple. It provides that:

Nothing in the information privacy principles applies in respect of—

- (a) The collection of personal information by an agency that is an individual; or
- (b) Personal information that is held by an agency that is an individual,—

where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs.

5.44 Most information privacy statutes in other countries have similar exemptions, although as discussed below there are some differences in the wording of the overseas provisions. The rationale of the exemption is clear enough – individuals should not have to comply with the Privacy Act in relation to everyday domestic activities such as taking photographs of friends and family or keeping records of family expenditure and activities. To routinely apply the Privacy Act to such activities would be both impractical and intrusive into people's personal and domestic lives. It could also see the Privacy Commissioner and the Human Rights Review Tribunal getting caught in the middle of domestic disputes. Nevertheless, the breadth of the exemption gives rise to significant concerns, particularly in the age of the internet, as discussed below.

5.45 The wording of section 56 refers only to information that is “collected or held” by an individual. In *S v P*, the Complaints Review Tribunal held that section 56 applies to use and disclosure of information, even though use and disclosure are not specifically referred to in the section.³⁹⁰

[W]e accept the submissions of the Privacy Commissioner that the information privacy principles concern **collecting** (principles 1–4) and **holding** (principles 5–11) information. The **protection, use or disclosure** of information concern obligations that can only arise if an agency **holds** information. There is therefore no need for s. 56 to specifically refer to those obligations because they are covered by the use of the word **hold** in s. 56(b). Section 56, therefore, also covers the disclosure of information.

Meaning of “personal affairs”

5.46 Paul Roth has raised questions about the meaning of “personal affairs” in section 56.³⁹¹ He notes that this expression has been contentious in Australian freedom of information legislation, and that courts in Australia have veered between broad and narrow interpretations of “personal affairs”. Roth asks, for example, whether information about a person's personal affairs can include information about his or her conduct at work? It could be desirable to clarify the meaning of “personal affairs”, although we recognise that it would be quite difficult to do this. We note that the words “personal affairs” are also used in principle 4(b)(ii).

390 *S v P* (12 March 1998) Complaints Review Tribunal 3/98, 4.

391 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA56.5.

Q73 Should the meaning of “personal affairs” in section 56 be clarified?
If so, how?

Scope of section 56

- 5.47 While there can be little doubt that an exemption along the lines of section 56 is necessary, it also creates a major gap in the protection offered by the Privacy Act. In our issues paper for Stage 3 of this Review we set out some hypothetical scenarios involving instances of surveillance. In relation to a number of these scenarios, we referred to the fact that a remedy might not be available through the Privacy Act because of section 56.³⁹² The question is whether the scope of section 56 can be narrowed while continuing to exclude the bulk of personal information collected or held in connection with personal, family or household affairs from the coverage of the privacy principles.
- 5.48 Some specific issues have been raised in relation to section 56. One concerns the use of section 56 where an individual has deliberately misled an agency, particularly in order to obtain information. For example, a person could obtain information about an individual by falsely claiming to be that individual or to have that individual’s consent. At present a complaint could be brought about the agency’s action in disclosing the information, but a complaint against the person who obtained the information under false pretences might well fail if that person could show that he or she obtained the information in connection with his or her personal or domestic affairs. Accordingly, the Privacy Commissioner recommended in *Necessary and Desirable* that section 56 should be amended so that an individual cannot rely on the domestic affairs exemption where that individual has collected personal information from an agency by falsely representing that he or she has the authorisation of the person concerned or is the person concerned.³⁹³
- 5.49 A second issue concerns the application of the section 56 exemption to activities that are unlawful. This issue has arisen in relation to intimate covert filming. At present there would be no remedy under the Privacy Act where, for example, a stepfather films his stepdaughter in the shower in a manner that would be in breach of the intimate covert filming provisions of the Crimes Act.³⁹⁴ We understand that there have been cases of this sort. Prior to the release of the Law Commission’s recommendations on intimate covert filming, the Privacy Commissioner recommended that the section 56 exemption should be limited so that it did not apply to intimate covert filming or to unlawful collection of personal information.³⁹⁵ The Law Commission subsequently recommended that section 56 be amended to provide that the domestic affairs exemption does not

392 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP 14, Wellington, 2009) 224–234; see scenarios 1–4, 12, 15.

393 *Necessary and Desirable* 224–226, rec 82.

394 Crimes Act 1961, ss 216G, 216H.

395 *3rd supplement to Necessary and Desirable*, rec 82A.

extend to “information obtained through criminal offending whether or not [the respondent has been] charged or convicted”.³⁹⁶ The Commission saw the Privacy Act as the best vehicle for providing a civil remedy for intimate covert filming.

5.50 The two issues discussed above are comparatively straightforward. There are, however, a range of other situations in which the section 56 exemption seems problematic, but the solutions are by no means clear. Consider the following scenarios:

- A and B have been in a sexual relationship, in the course of which A has taken intimate photographs of B with her consent. When the relationship breaks up, A posts these photos on a publicly-accessible website without B’s consent.
- C and D are university students who attend a wild party. C takes photographs of the party, which she puts on her page on a social networking site. One of the photographs shows D in a drunken and undignified state. The photographs are later seen by a prospective employer, and D is not employed as a result.
- E writes a blog, much of which is concerned with her everyday life and her interactions with friends and family. She mentions in the blog that a friend is having an affair. Although she does not name the friend, his identity is apparent from the context to those who know him.

In each of these cases, it is likely that the individual who has (arguably) breached another person’s privacy could successfully use the section 56 exemption.

5.51 Each of these scenarios also involves information being made available online. Although the issues concerning section 56 do not arise only from the internet, the internet does create new problems when material relating to “personal, family or household affairs” is made available to a much wider audience. It is arguable that making the material more widely available by placing it on the internet takes it out of the personal, family or household sphere, but this is by no means clear, particularly if access to the site in question is restricted to some degree. For an increasing number of people, websites are the modern equivalents of diaries or family photo albums.

5.52 It may be that there is no realistic way of restricting the scope of section 56 without rendering it ineffective. A recent article on data protection laws and online social networking by Gehan Gunasekara and Alan Toy argues that the section 56 exemption should be given a fairly wide reading and that an individual’s motives for collecting, using or disclosing information should not affect that individual’s ability to rely on this exemption.³⁹⁷

5.53 If it is considered desirable to restrict the scope of section 56, one option would be to modify the wording of the section. Section 56 refers to personal information that is held “*solely or principally* for the purposes of, or in connection with” a person’s personal, family or household affairs. By contrast, overseas statutes use phrases like:

396 New Zealand Law Commission *Intimate Covert Filming* (NZLC SP15, Wellington, 2004) 37.

397 Gehan Gunasekara and Alan Toy “‘MySpace’ or Public Space: The Relevance of Data Protection Laws to Online Social Networking” (2008) 23 NZULR 191, 213.

- “*only* for the purposes of”;³⁹⁸
- “*only* for the purposes of, or in connection with”;³⁹⁹
- “personal information that the individual collects, uses or discloses for personal or domestic purposes *and does not collect, use or disclose for any other purpose*”;⁴⁰⁰
- “*concerned only with the management of his personal, family or household affairs*”;⁴⁰¹ and
- “in the course of a *purely* personal or household activity”.⁴⁰²

Thus, overseas legislation seems to be more tightly confined to collection, use or disclosure that is only for personal, household or family purposes and for no other purposes.

5.54 A second approach would be to expressly exclude certain matters from the coverage of section 56 (as with the proposals discussed above to exclude misleading or criminal conduct). For example, the statute could provide that section 56 does not apply where:

- The person collecting, using or disclosing personal information knows that the person to whom that information relates has refused consent for such collection, use or disclosure. The person concerned would probably have to clearly indicate a refusal of consent, and there would not be a positive onus on the person collecting, using or disclosing the information to seek consent.
- The person collecting, using or disclosing the information has malicious motives for doing so.
- The person collecting, using or disclosing the information does so at least in part in order to obtain some financial benefit.
- The collection, use or disclosure is “highly offensive”, or causes harm in one of the forms referred to in section 66(1)(b) of the Act.

Such amendments might help to deal with some problematic cases. However, they might still not assist in, for example, the case of a person posting embarrassing photographs of another on a social networking site, unless a malicious motive, a refusal of consent, or identifiable harm could be demonstrated.

5.55 A third, and more far-reaching option, would be not to treat personal, family and household affairs purposes as an exemption. Instead, the Commissioner and the Tribunal could be required to give due weight, in dealing with complaints against individuals, to the fact that the information in question was collected or held for the purposes of personal, family or household affairs. This would essentially mean balancing the privacy interests of the individual to whom the information relates against the interests of other individuals in the autonomous management of their personal and domestic affairs. Individuals would become subject to the privacy principles even in relation to their personal and domestic

398 Data Protection Act 1998 (UK), s 36.

399 Privacy Act 1988 (Cth), s 16E.

400 Personal Information Protection and Electronic Documents Act SC 2000 c 5, s 4(2)(b).

401 Personal Data (Privacy) Ordinance (Hong Kong), s 52(a).

402 European Union Directive 95/46/EC, art 3(2).

affairs, but they would be given a significant amount of leeway in complaints. The Privacy Commissioner could also issue guidelines to assist individuals in understanding how the Privacy Act applies to them. Such a change might, nonetheless, give rise to significant uncertainty, and leave the Privacy Commissioner and the Tribunal having to make some very difficult judgements.

- 5.56 We propose that the section 56 exemption should not apply where information is obtained by misleading or unlawful conduct. With regard to the wider issues about the scope of section 56, our preliminary view is that the section 56 exemption should not apply where the actions of the person seeking to rely on the exemption cause harm to another person or persons. Harm could be defined in the terms currently set out in section 66(1)(b) of the Act. In chapter 8 we propose to remove the harm threshold for complaints. If the proposal to remove the harm threshold results in the deletion of section 66(1)(b), the wording of that provision could be included (with necessary modifications) in section 56.

Q74 We propose that section 56 should be amended to provide that it does not apply where a person has collected information from an agency by engaging in misleading conduct (in particular, by falsely claiming to have the authorisation of the individual to whom the information relates or to be that individual). Do you agree?

Q75 We propose that section 56 should be amended so that it does not apply where personal information is obtained unlawfully (whether or not the person obtaining the information has been charged or convicted of a criminal offence). Do you agree?

Q76 We propose that section 56 should be amended so that it does not apply where the collection, use or disclosure of personal information results in identifiable harm to another individual. Do you agree? If not, do you support any of the other options discussed in paragraphs 5.53–5.55?

Q77 Do you have any other suggestions for amending section 56?

Section 57– intelligence agencies

5.57 Section 57 provides that principles 1 to 5 and 8 to 11 do not apply to information collected, held, obtained, used or disclosed by, or disclosed to, an intelligence organisation. In other words, only the access, correction and unique identifier principles apply to these organisations. Section 2 defines “intelligence organisation” as meaning the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB).

5.58 Section 57 and other special provisions in relation to the intelligence organisations (discussed below) recognise the unique nature of the work of the security and intelligence agencies. Some of the distinctive features of their work have been summarised by the NZSIS:⁴⁰³

- Security investigations are long-term and do not always have a clear end point, in contrast to law enforcement investigations which typically end with the laying of charges.
- Security investigations are “prospective in nature, with the primary emphasis on prevention”.
- Intelligence is collected covertly from human sources and by means of surveillance devices.

The exemptions in the Privacy Act in relation to the intelligence organisations allow them to continue to operate covertly and to protect their sources and methods.

5.59 At the same time, the work of the intelligence organisations clearly has significant implications for privacy, which is why they are not exempted entirely from the Act and why they are subject to oversight not only by the Privacy Commissioner but also by the Inspector-General of Intelligence and Security (as discussed below). The Privacy Commissioner’s view is that:⁴⁰⁴

- the intelligence organisations’ roles should be restricted to a tight brief and should not “stray into areas which can be appropriately managed by normal and open governmental and policing activities”;
- while much of the organisations’ work will need to be conducted in secret, there will be areas in which information can be disclosed publicly, to the individuals concerned or to oversight bodies;
- the organisations should be subject to similar accountability mechanisms to other agencies (albeit sometimes in a modified manner), except where there is a good reason for this not to occur; and
- where the organisations unjustifiably breach individual rights, including the right to privacy, redress should be available.

403 New Zealand Security Intelligence Service “Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS” www.nzsis.govt.nz (accessed 19 January 2010) paras 8–12.

404 *Necessary and Desirable* 224. The current Privacy Commissioner takes the same view: see Marie Shroff “Linking Intelligence to Provide Value: Personal Information, Privacy and the Information Century” (speech to Institute of Intelligence Professionals Conference, Wellington, 25 August 2009).

Access requests and use of the “neither confirm nor deny” response

- 5.60 Section 27 of the Privacy Act allows information requested pursuant to principle 6 to be withheld if disclosure of the information would be likely to prejudice the security or defence of New Zealand, the maintenance of the law, and other related interests. Section 32 provides that, where an access request pursuant to principle 6 relates to information to which section 27 “applies, or would, if it existed, apply”, and where the interest protected by section 27 would be prejudiced if the existence or non-existence of the information were to be disclosed, the agency responding to the request may give written notice to the applicant that it neither confirms nor denies the existence or non-existence of that information.
- 5.61 The NZSIS often relies on the ability to neither confirm nor deny under section 32, and has set out its reasons for doing so. It explains that “a request for information to the NZSIS is tantamount to asking whether there is or has been an investigation by the NZSIS into the individual or the subject matter.” Furthermore, neither confirming nor denying the existence or non-existence of information may be necessary to avoid disclosing the existence of a covert source. While it might seem that there would be no harm in confirming that no information is held, the NZSIS maintains that confirming the non-existence of information can prejudice security by disclosing what the Service does not know or is not investigating.⁴⁰⁵ In particular, it states that:⁴⁰⁶
- Not knowing whether the NZSIS is investigating a particular activity or not has something of a deterrent effect. If it becomes a simple exercise to identify what is not of interest to the NZSIS, the benefit of the deterrent effect is lost.
 - If a correspondent is undertaking activities of security concern, and receives a “no information held” response for a subject they believed should be under investigation, they now know they have not been detected.

Processes for privacy complaints against the intelligence organisations

- 5.62 Section 81 of the Privacy Act sets out a special procedure relating to privacy complaints against the intelligence organisations (bearing in mind that these can only be complaints of breaches of principles 6, 7 or 12). Where, after investigating a complaint against an intelligence organisation, the Privacy Commissioner considers that there appears to have been an interference with the privacy of an individual, the Commissioner shall report that opinion, and the reasons for it, to the relevant intelligence organisation. The Commissioner may also make recommendations, and may request that the organisation report to the Commissioner within a reasonable time on the steps (if any) that it proposes to take to comply with the Commissioner’s recommendations. If, within a reasonable time after receiving that report, the Commissioner considers that the organisation has not taken adequate steps to address the issue, the Commissioner may send a copy of the report and recommendations to the Prime Minister, who may lay part or all of the report before the House of Representatives. Section 81(6) provides that sections 76 and 77 (concerning

405 New Zealand Security Intelligence Service “Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS” www.nzsis.govt.nz (accessed 19 January 2010) paras 13–18.

406 New Zealand Security Intelligence Service “Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS” www.nzsis.govt.nz (accessed 19 January 2010) para 19.

compulsory conferences and procedures following the Privacy Commissioner's investigation of a complaint), and all of the sections concerning proceedings before the Human Rights Review Tribunal, do not apply to complaints against intelligence organisations. In other words, complaints against intelligence organisations cannot proceed to the Tribunal.

- 5.63 In parallel with the above procedures, people can also complain about breaches of privacy by intelligence organisations to the Inspector-General of Intelligence and Security. The functions of the Inspector-General include inquiring on his or her own motion, or at the request of the Minister, into any matter that relates to compliance by intelligence agencies with the law; and inquiring into any complaint by a New Zealander concerning an act or omission of an intelligence agency that may have adversely affected the complainant.⁴⁰⁷ This would seem to allow the Inspector-General to investigate privacy matters that go beyond those that can be investigated by the Privacy Commissioner – for example, the Inspector-General could investigate a complaint that a person has been adversely affected by a disclosure of personal information by an intelligence organisation. The Inspector-General may consult with the Privacy Commissioner in relation to any matter relating to the Inspector-General's functions, and likewise the Privacy Commissioner may refer complaints to the Inspector-General and consult with the Inspector-General.⁴⁰⁸

Extending other privacy principles to the intelligence organisations

- 5.64 In *Necessary and Desirable*, the Privacy Commissioner recommended that the exemption in section 57 should be narrowed so that principles 1, 5, 8 and 9 apply to the intelligence organisations.⁴⁰⁹ The Commissioner was of the view that these principles “provide a sound basis for fair information handling and have clear relevance to intelligence organisations”, and that they would not need to be amended to establish any national security exception.⁴¹⁰ Submissions were overwhelmingly in favour of applying these principles to the intelligence organisations. The NZSIS and the GCSB had no objections to an amendment to the Privacy Act to make them subject to principles 1, 5, 8 and 9. The two intelligence organisations did enter a caveat with regard to principle 9, noting that it is often necessary to retain intelligence information for future purposes. They did not, however, appear to be arguing for an amendment or exception to principle 9, but rather for flexibility in its application to intelligence organisations. The NZSIS and GCSB also expressed a preference for oversight of compliance with these principles to be carried out by the Inspector-General rather than the Privacy Commissioner. The intelligence organisations made clear in their submissions that they considered it essential that they continue to be exempted from principles 2, 3, 4, 10 and 11.⁴¹¹

407 Inspector-General of Intelligence and Security Act 1996, s 11(1)(a) and (b).

408 Inspector-General of Intelligence and Security Act 1996, s 12(2); Privacy Act 1993, ss 72B, 117B. Section 15(3) of the Inspector-General of Intelligence and Security Act 1996 provides that nothing in section 12 of that Act limits the powers, duties and responsibilities of the Privacy Commissioner.

409 *Necessary and Desirable* 224–229, rec 83.

410 *Necessary and Desirable* 226.

411 New Zealand Security Intelligence Service, submission to the Office of the Privacy Commissioner, 2 December 1997; Government Security Communications Bureau, submission to the Office of the Privacy Commissioner, 31 October 1997.

Q78 Should principles 1, 5, 8 and 9 apply to the intelligence organisations?

Q79 Should there be any other changes to the exemption for the intelligence organisations under section 57?

Q80 Should there be any changes to the procedures for investigating privacy complaints involving the intelligence organisations? Are any problems created by the dual jurisdiction of the Privacy Commissioner and the Inspector-General of Intelligence and Security?

POSSIBLE NEW EXEMPTIONS 5.65 The Law Commission is not aware of a need for any new exemptions to be included in the Act, but submitters are welcome to propose new exemptions.

Q81 Should any new exemptions be included in the Privacy Act?