

# Chapter 3

## Key definitions

- 3.1 Section 2 of the Privacy Act defines various terms used in the Act. Some of these terms are discussed elsewhere in this issues paper. Here we discuss three key terms that are central to the scope and coverage of the Act as a whole: “personal information”, “individual” and “collect”. At the end of the chapter we ask whether there are any other terms whose meaning for the purposes of the Act should be amended or clarified.

### “PERSONAL INFORMATION”

- 3.2 The definition of “personal information” in the Privacy Act is very broad, and is not limited to information that is particularly sensitive, intimate or private. Nor does the Act have a separate category of “sensitive information”, as some overseas privacy legislation does. The Act defines personal information as “information about an identifiable individual”. It goes on to state that the definition includes information about a death maintained pursuant to the Births, Deaths, Marriages and Relationships Registration Act 1995 (as discussed later in the chapter). “Individual” is separately defined, and is discussed in a later section of this chapter.
- 3.3 The definition of personal information is central to establishing the scope of the Privacy Act, yet Katrine Evans has commented that “deciding what is, and what is not ‘personal information’ can be one of the hardest legal calculations in everyday privacy practice.”<sup>126</sup> It is important to emphasise at the outset, however, that in most cases it will be quite clear whether information is “personal information” or not. We are not aware of the definition of personal information causing major problems in the day-to-day application of the Act by agencies. Ambiguity and uncertainty arise only at the margins; but those margins can be very important in particular cases, and for establishing the boundaries of the Act’s coverage. In this section we ask: to what extent is the definition of “personal information” inherently complex and ambiguous, and to what extent could it be clarified in the statute or by some other means? Some areas of ambiguity are discussed below.

<sup>126</sup> Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner “Personal Information in New Zealand: Between a Rock and a Hard Place?” (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 1.

## “Information”

- 3.4 “Information” is not defined in either the Privacy Act or the Official Information Act 1982 (OIA). The leading New Zealand authority on the meaning of information is the definition given by McMullin J in *Commissioner of Police v Ombudsman*: “that which informs, instructs, tells or makes aware”.<sup>127</sup> To constitute information, something must be capable of being understood; a person must be able to derive meaning from it. Some writers have drawn a distinction between “data” and “information”. Raymond Wacks writes that: “‘Data’ become ‘information’ only when they are communicated, received, and understood. ‘Data’ are therefore potential ‘information’.”<sup>128</sup> Paul Roth draws a similar distinction, writing that:<sup>129</sup>

“information” may be contrasted to mere “data” in that information is always “about” something or someone, while data are the raw material or building blocks that comprise “information”. Information can therefore be conceived of as “data” that have been “processed” in some way, and the essence of “information” is that it conveys meaning or, as one author has termed it, “aboutness”. Information can be viewed as data placed in context and made meaningful or useful in some way.

There is something to this distinction, although we would caution against attaching any significance to the fact that the New Zealand Privacy Act is concerned with “personal information” while some overseas statutes (particularly in Europe) use the term “personal data”: we think both terms are generally used to mean the same thing in information privacy laws around the world.<sup>130</sup>

- 3.5 It seems to be undisputed that “personal information” covers information collected or held in a wide range of forms, including audio and visual recordings. We believe that it does not cover bodily samples (as distinct from information obtained from those samples), as discussed further below.
- 3.6 Personal information for the purposes of the Privacy Act is not limited to information that has been recorded in some form, and most of the authority in cases relating to the OIA, the Local Government Official Information and Meetings Act 1987 and the Privacy Act is that unrecorded matter held in a person’s mind can be “information”.<sup>131</sup> The inclusion of information that exists only in a person’s mind appears to set the New Zealand Privacy Act apart from most overseas privacy legislation. For example, the definition of “data” in the Data Protection Act 1998 (UK) is limited to information which is recorded or is being automatically processed by machine (which implies that it must exist in some sort of record recognisable by the machine).<sup>132</sup> The definition of “personal information” in the Privacy Act 1988 (Cth) expressly states that it includes

127 *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 402 (CA) McMullin J.

128 Raymond Wacks *Personal Information: Privacy and the Law* (Clarendon Press, Oxford, 1989) 25.

129 Paul Roth “What is Personal Information?” (2002) 20 NZULR 40, 51.

130 Indeed, the Data Protection Act 1998 (UK), s 1(1), defines “data” as meaning certain types of “information”.

131 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,203–152,207.

132 Data Protection Act 1998 (UK), s 1(1).

information “whether recorded in a material form or not”,<sup>133</sup> but this provision is limited by other provisions in the Act which restrict the Act’s application to information that is being collected for inclusion in a “record”, or is held in a “record”.<sup>134</sup> In New South Wales, the Privacy and Personal Information Act 1998 similarly states that “personal information” includes information “whether or not recorded in a material form”,<sup>135</sup> and the Act’s application is not limited in the same way as is the Federal Act’s. This opened the door for both the Administrative Decisions Tribunal and that Tribunal’s Appeal Panel to find that personal information could include information held in a person’s mind. However, this finding was overturned on appeal to the Court of Appeal, with Spigelman CJ holding that:<sup>136</sup>

Of particular significance is the body of consecutive sections between s12 and s19 of the Privacy [and Personal Information] Act which adopt as their criterion of operation a reference to where a public sector agency “holds personal information” .... It is almost impossible to conceive how almost all of those ... sections could operate in practice if they were intended to apply to information in the minds of employees acquired by direct visual or aural experience and never recorded in any manner.

- 3.7 The New South Wales Court of Appeal decision raises some interesting questions about the implications of treating information held in a person’s mind as personal information for the purposes of the Privacy Act. On the one hand, knowledge and opinions held in a person’s mind are clearly information, and treating them as such for the purposes of the Act enhances people’s rights under the Act. For example:
- When people seek access to information about themselves held by an agency (principle 6), that information may include material that has not been recorded but does nonetheless influence an agency’s dealings with an individual. Indeed, excluding undocumented information could create an incentive for agencies not to keep a record of meetings or other interactions that concern a particular individual, or to destroy such records.
  - Principle 11 deals with disclosure of personal information. Disclosure of information that is not contained in a recorded form can be just as harmful as disclosure of information in writing, in a photograph, or in another type of document.
  - The requirement to check the accuracy of personal information before use (principle 8) is just as important if that information is held in a person’s mind as it would be if the information were recorded in some way.
- 3.8 On the other hand, there are some conceptual and, perhaps, practical difficulties with including information held in a person’s mind in the Act’s coverage. For example:
- How can the purpose for which such information is held be established?
  - How can the security of such information be protected (principle 5)?
  - If such information is incorrect, how can it be corrected (principle 7)?
  - How can an agency ensure that the information is not kept for longer than is necessary (principle 9)?

---

133 Privacy Act 1988 (Cth), s 6(1).

134 Privacy Act 1988 (Cth), ss 14, 16B.

135 Privacy and Personal Information Act 1998 (NSW), s 4(1).

136 *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192, para 28.

- 3.9 Some of these difficulties may be more theoretical than real, and a number of features of the Act help to deal with any potential problems. In particular:
- A number of the privacy principles require agencies to take only such action as is reasonable in the circumstances.
  - Information held in the mind of an individual will not necessarily be held by the agency for which that individual works or of which that individual is a member.<sup>137</sup>
  - With regard to access requests under principle 6, a request may be refused if the information “is not readily retrievable” or “cannot be found”.<sup>138</sup> This may sometimes be the case where information held in a person’s mind is concerned.
- 3.10 Nonetheless, evidential problems may arise, as Paul Roth notes:<sup>139</sup>

Once it is accepted that the Privacy Act covers information that is not in documentary form, evidential issues will inevitably arise in relation to whether personal information is actually held; whether it is “readily retrievable”; whether it has been fully disclosed in response to a Principle 6 request; and whether it has been disclosed in breach of Principle 11.

In *A and A v G*, the Complaints Review Tribunal considered a complaint involving information disclosed in the course of a conversation. The Tribunal commented that the definition of personal information in the Act:<sup>140</sup>

carries within it the specific implication that the information the subject of any issue raised by the Act is itself known, accepted or understood in very precise terms. This will generally not pose a problem where the information at issue is recorded in some way. There is, however a difficulty when the precise nature of the personal information is not known, accepted, or understood in precise terms. That is a difficulty which is likely to arise in respect of personal information which is not recorded but which is held in the memory of an individual.

- 3.11 The Law Commission would be interested to hear, as part of submissions on the definition of “personal information”, whether the inclusion of information held in a person’s mind in the definition of personal information causes practical problems for agencies, and whether such information should continue to be covered by the definition.
- 3.12 Other questions are whether information includes opinions and false information. With regard to false information, it seems clear that this is covered by the Privacy Act, and that whatever limitations there may be with regard to the privacy tort’s coverage of false information do not apply in the Privacy Act context. If false information did not fall within the coverage of “personal information”, principle 7 (which concerns correction of inaccurate information) would be nonsensical. There also seems to be no reason why opinions cannot be information, although they are not expressly included in the definition of personal information.

137 Privacy Act 1993, ss 3–4.

138 Privacy Act 1993, s 29(2)(a) and (b); see also the terms of principle 6 itself.

139 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,401.

140 *A and A v G* (13 July 1999) Complaints Review Tribunal 18/99, 6.

3.13 The fact that the Privacy Act contains no definition of “information” does not seem to have created significant problems. However, it could be worthwhile to put certain matters beyond doubt by amending the definition of “personal information” to include elements found in the Privacy Act 1988 (Cth):<sup>141</sup>

- “information or an opinion”;
- “whether true or not”; and
- “whether recorded in a material form or not” (although we believe that a better form of words for the New Zealand Act would be “whether recorded in a document or not”, since “document” is fully defined in the Act).

It is also worth noting that the definition of “personal information” in the Privacy of Personal Information Bill recently introduced in South Africa expressly includes both “the personal opinions, views or preferences of the person” and “the views or opinions of another individual about the person”.<sup>142</sup>

### “About”

3.14 Whether information is “about” an identifiable individual or not is probably the question that gives rise to the most uncertainty in the application of the definition of “personal information”. It also appears to be the most difficult issue to resolve or clarify through amending the statute. Questions concerning whether information is “about” an individual seem to arise most commonly in access cases, where decisions have to be made about whether particular information is personal information about the requestor that should therefore be released to him or her. However, they can also arise in cases concerning breaches of other privacy principles.

3.15 In obiter comments in *Harder v Proceedings Commissioner*, the majority in the Court of Appeal appeared inclined to read down the meaning of “personal information” by limiting it to information that is “about” an individual in a fairly narrow sense.<sup>143</sup> There is no authoritative decision on this point in New Zealand, but an indication of how the courts could narrow the scope of personal information by reference to the requirement that the information be “about” an individual can be found in the English case of *Durant v Financial Services Authority*. In that case, the Court of Appeal held that whether or not mention of a data subject in a document amounts to his personal data in any particular instance “depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree”. The Court stated that two notions could be of assistance in this respect:

---

141 Privacy Act 1988 (Cth), s 6. The ALRC has recommended keeping these aspects of the definition of “personal information” unchanged: Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 306, 309 (rec 6–1).

142 Protection of Personal Information Bill (South Africa), cl 1, definition of “personal information”, subclauses (e) and (g).

143 *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, paras 23–24 (CA) Tipping J; however, see the contrary view of Gault J at para 49. The Court’s obiter comments on the meaning of “personal information” have been questioned by some commentators: see Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner “Personal Information in New Zealand: Between a Rock and a Hard Place?” (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 5; Paul Roth “What is Personal Information?” (2002) 20 NZULR 40, 43–45.

- whether the information “is biographical in a significant sense”, that is, whether it has personal connotations and could compromise his or her privacy, or merely records his or her involvement in some matter or event; and
- whether the information has the individual as its focus, or whether it actually has as its focus some other person with whom the individual may have been involved or some event in which he or she may have figured or had an interest.

“In short,” the Court concluded, “it is information that affects his privacy, whether in his personal or family life, business or professional capacity.”<sup>144</sup> This narrow interpretation of the meaning of “personal data” has been criticised by a number of commentators.<sup>145</sup>

- 3.16 In technical guidance on the meaning of personal data,<sup>146</sup> the UK Information Commissioner has attempted to reconcile the finding of the Court in *Durant* with the much broader definition of personal data in an Opinion of the European Union Article 29 Data Protection Working Party.<sup>147</sup> The Article 29 Working Party Opinion distinguishes between three elements which, if any one of them is present, indicate that data “relate” to an individual (which is the terminology of the EU Data Protection Directive). Only one of these elements, the “content” element, concerns whether the information is “about” an individual in the sense that it involves his or her personal details, characteristics, activities and so on. The other two elements concern whether the information will be used to evaluate, treat in a certain way, or influence the status or behaviour of an individual; or whether the use of the information is likely to have an impact on an individual’s rights or interests.<sup>148</sup>
- 3.17 With the exception of the obiter comments in *Harder*, New Zealand courts and the Human Rights Review Tribunal have not so far shown any inclination to take the narrow approach of the English Court of Appeal in *Durant*. However, a distinction between information “about” an individual and information that in some way relates to an individual was drawn by the Human Rights Review Tribunal in *CBN v McKenzie Associates*. While declining to draw any final conclusions about the scope of “personal information”, the Tribunal commented that “The fact that information may become relevant to someone does not necessarily convert it into information ‘about’ that person.” In the particular case in question, information about the plaintiff’s wife held on the defendants’ file “may have been relevant to the plaintiff in the sense that it might have either

144 *Durant v Financial Services Authority* [2003] EWCA Civ 1746, para 28 Auld LJ.

145 See, for example, David Lindsay “Misunderstanding ‘Personal Information’: *Durant v Financial Services Authority*” [2004] PLPR 13.

146 *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner’s Office, 2007).

147 Richard Cumbley and Peter Church “EU – What is Personal Data?” (October 2008) *Technology, Media & Telecommunications News* www.linklaters.com (accessed 30 July 2009). The UK Information Tribunal has commented that it has “difficulty in reconciling the approach in the Guidance with that in *Durant*”: *Harcup v Information Commissioner and Yorkshire Forward* (5 February 2008) Information Tribunal (UK) EA/2007/0058, para 20.

148 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 10–11.

limited or enhanced his chances of obtaining the custody arrangements that he wanted”, but the Tribunal “struggle[d] to see” that that information thereby became information “about” the plaintiff.<sup>149</sup>

3.18 Examples of difficult questions with regard to when information is “about” an individual include:<sup>150</sup>

- Are exam scripts information about the students who wrote them? What about the exam questions – in responding to an access request, can an agency legitimately provide copies of the answers without the questions?
- Assuming that opinions are “information”, is A’s opinion of B personal information about A, about B, or about both of them?
- In what circumstances can information about other people be information about an individual? If information about another person is relevant to a decision that is made about person A, does that make it information about person A? (For example, information about the successful candidate for a job for which A applied unsuccessfully.)
- In what circumstances can information about an object be information about a person? (For example, an insurance report about a mechanic’s repairs to a person’s car, in the context of a dispute over the adequacy of the repairs.)
- If an agency has a file about an individual, should everything in that file be considered to be about the individual, or can it properly be separated into information that is about the individual and information that is not?
- To what extent, and in what circumstances, are minutes of meetings information about the participants in the meeting?

3.19 The answer to questions such as these seems to be: it all depends on the context. The Human Rights Review Tribunal acknowledged as much in *CBN v McKenzie Associates*:<sup>151</sup>

there is no “bright line” test which separates that which is obviously personal information about an identifiable individual from that which is not. Much will depend in any given case on the context in which the information is found.

It seems unlikely that it would be either possible or desirable to amend the definition of “personal information” to provide clarification with regard to what makes something information “about” an individual. Guidance from the Privacy Commissioner, like that produced by the Information Commissioner in the UK, is an option that could be considered, however.

---

149 *CBN v McKenzie Associates* [2004] NZHRRT 48, para 39.

150 For further discussion of these and other examples see Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner “Personal Information in New Zealand: Between a Rock and a Hard Place?” (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 8–9; Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12; Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 9–12; *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner’s Office, 2007) 9–17.

151 *CBN v McKenzie Associates* [2004] NZHRRT 48, para 41.

### “Identifiable”

- 3.20 It is significant that the definition of personal information requires only that the individual be “identifiable”, not that he or she be “identified” in the information. Even so, there could be a question as to whether the individual must be identifiable from the internal evidence of the information in question alone, or whether the individual could be identifiable from the information in question in combination with other information. According to Paul Roth, the Ombudsmen, the Privacy Commissioner and the courts have taken the latter approach to the question of identifiability. Roth further argues that the approach of not requiring that individuals be identifiable from the information in question alone is consistent with overseas legislation and international standards, and is supported by certain features of the Privacy Act itself.<sup>152</sup>
- 3.21 If it is accepted that this approach is the right one, at least two areas of uncertainty remain. First, by whom must the individual be identifiable? Must the individual be identifiable to casual observers, or is it enough that he or she could be identified by close friends or family? What if the individual can only be identified by himself or herself? It seems that the individual does not necessarily have to be identifiable to the world at large, and it can be enough that he or she can be identified by those who know him or her. In *Proceedings Commissioner v Commissioner of Police*, the Complaints Review Tribunal did not accept the argument:<sup>153</sup>

that an identifiable individual’s privacy should not be regarded as breached if an identification can only be made as a result of prior knowledge by some members of the public of an individual. We think this would limit identifiability to identification by strangers and we do not accept that this is what the definition of personal information says.... It is enough that they are able to be identified by anyone who can make an identification as the result of the receipt of personal information not previously known.

Where the individual can be identified only by himself or herself, the Privacy Commissioner has formed the opinion that there is no personal information involved.<sup>154</sup> However, Paul Roth argues that this view is mistaken: in such a case the information can still be personal information, and the fact that no one else can identify the individual should instead be taken into account when assessing the question of harm.<sup>155</sup>

- 3.22 The second area of uncertainty concerns the means and practicality of identification. In other words, is it reasonably practicable, rather than merely theoretically possible, to identify the individual? Some international instruments,

152 Paul Roth “What is Personal Information?” (2002) 20 NZULR 40, 48–50.

153 *Proceedings Commissioner v Commissioner of Police* (16 December 1999) Complaints Review Tribunal 37/99.

154 *Man Complains About Publication of his Photograph in a Booklet* [2006] NZPrivCmr 7 – Case Note 64131; Katrine Evans, Assistant Commissioner (Legal), Office of the Privacy Commissioner “Personal Information in New Zealand: Between a Rock and a Hard Place?” (paper presented to Interpreting Privacy Principles: Chaos or Consistency? symposium, Sydney, 2006) 3.

155 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.12, 152,404–152,405.

and legislation and guidance from other jurisdictions, provide greater assistance with regard to this question than does the New Zealand Privacy Act. For example:

- The definition of personal data in the Hong Kong Personal Data (Privacy) Ordinance refers to information from which an individual's identity can "practicably" be directly or indirectly ascertained.<sup>156</sup> Likewise, some Australian statutes refer to information from which a person's identity can "reasonably" be ascertained.<sup>157</sup>
- The Data Protection Act 1998 (UK) refers to data relating to an individual who can be identified from the data alone, or from the data "and other information which is in the possession of, or is likely to come into the possession of, the data controller".<sup>158</sup>
- Recital 26 of the EU Data Protection Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the [data] controller or by any other person to identify the said person".<sup>159</sup>
- Elaborating on the statement in the EU Directive, guidance from the UK Information Commissioner states that "the fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the data subject is identified is not sufficient to make the individual identifiable for the purposes of the Directive." However, assessing identifiability does not involve simply considering the means reasonably likely to be used by the average person in the street, "but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals".<sup>160</sup>

3.23 Similar statements, either in the Privacy Act or in guidance from the Privacy Commissioner, could assist in New Zealand. Assistance could also be provided by listing some factors to be taken into account in assessing the practicality of ascertaining a person's identity. Microsoft Asia Pacific, in a submission to the Australian Law Reform Commission (ALRC), stated that the reasonableness test:<sup>161</sup>

necessitates a consideration of the cost, difficulty, practicality and likelihood of the organisation linking information with other personal information accessible to it, and not merely whether the organisation would be able to link the information after incurring substantial expenditure.

---

156 Personal Data (Privacy) Ordinance (Hong Kong), s 2.

157 Privacy Act 1988 (Cth), s 6; Privacy and Personal Information Act 1998 (NSW), s 4; Information Privacy Act 2000 (Vic), s 3.

158 Data Protection Act 1998 (UK), s 1(1).

159 EC Directive 95/46/EC.

160 *Data Protection Technical Guidance: Determining What is Personal Data* (UK Information Commissioner's Office, 2007) 7.

161 Microsoft Asia Pacific, submission to the ALRC, quoted in *Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 301; at 308 the ALRC states that this "is an appropriate formulation of the test".

Similarly, a Council of Europe Recommendation states that: “An individual shall not be regarded as ‘identifiable’ if the identification requires an unreasonable amount of time, cost and manpower.”<sup>162</sup>

- 3.24 The issue of identifiability is further complicated by the increasing ease with which anonymised or deidentified information can be reidentified. Computers have made it easier to analyse data and find unique “data fingerprints” within it, but perhaps even more importantly the internet has made a vast amount of data readily available, so that data fingerprints can be combined with other information in order to identify the individuals to whom those fingerprints correspond. In a recent article, American legal academic Paul Ohm has argued that, as a result of advances in reidentification, the concept of “personally-identifiable information” (PII) on which laws like the Privacy Act depend has been rendered meaningless. PII is an ever-expanding category, according to Ohm, and should therefore be rejected as a basis for information privacy regulation. Instead, he argues, privacy law should be based on assessing risks of harm in specific contexts and weighing those risks against the benefits of free flows of information in those contexts.<sup>163</sup> Ohm’s article is a major challenge to one of the key concepts underlying information privacy law around the world, and the problems he identifies will probably become more acute over time.

*A particular issue: Internet Protocol (IP) addresses*

- 3.25 As with other elements of the definition of personal information, context will often be very important in determining whether or not a piece of information is linked to an identifiable individual. One example of the importance of context is the issue of whether an Internet Protocol (IP) address can be information about an identifiable individual, a question about which there has been much debate. Strictly speaking, an IP address identifies a computer or other internet-connected device, not a person (just as, strictly speaking, a street address identifies a house, not the owner or inhabitant of the house). On its own, therefore, an IP address could be considered not to constitute personal information. IP addresses can be static (that is, the address stays the same each time the user connects to the internet) or dynamic (meaning that the address changes each time the user connects to the internet). Regardless of whether the address is static or dynamic, the Internet Service Provider (ISP) will know the identity of the person or organisation holding the subscriber account to which the IP address has been assigned (although that person may not be the user at any given time).<sup>164</sup> It is also arguable that, even if the user’s identity as a living individual is not known, his or her online activity is identifiable by means of the IP address for purposes such as targeting of online advertising.<sup>165</sup>

162 Council of Europe Recommendation on Communication to Third Parties of Personal Data Held by Public Bodies (9 September 1991) R(91)10, quoted in Paul Roth “What is Personal Information?” (2002) 20 NZULR 40, 50.

163 Paul Ohm *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (University of Colorado Law Legal Studies Research Paper No 09–12, 2009), available at [www.ssrn.com](http://www.ssrn.com).

164 Rosemary Jay and Louise Townsend “IP Addresses and the Data Protection Act” (March 2008) [www.out-law.com](http://www.out-law.com) (accessed 29 July 2009).

165 “Hustinx: Nameless Data Can Still be Personal” (6 November 2008) [www.theregister.co.uk](http://www.theregister.co.uk) (accessed 29 July 2009).

- 3.26 There have been a range of views on whether an IP address is personal information. Some decisions in overseas jurisdictions have held that IP addresses are not personal information because they do not directly identify individuals.<sup>166</sup> The Article 29 Data Protection Working Party, on the other hand, considers that IP addresses are data relating to identifiable individuals. The Working Party acknowledges that in some cases (such as computers at internet cafes), the individual using the computer will truly not be identifiable from the IP address, but considers that unless an ISP is in a position to know with certainty that particular data corresponds to unidentifiable users it should treat all IP information as personal data, “to be on the safe side”.<sup>167</sup> The ALRC takes a middle-ground position, arguing that information that would allow an individual to be contacted (such as a phone number, street address or IP address in isolation) is not personal information, but that “such information may come to be associated with a particular individual as information accretes around the number or address.”<sup>168</sup> It seems that whether an IP address is personal information or not is a matter that can only be decided in relation to the particular context in which that address is collected, held, used or disclosed. It is probably not a matter that can be clarified by an amendment to the Privacy Act, although guidance from the Privacy Commissioner could be considered.

### Options for clarifying the definition of “personal information”

- 3.27 There are three options for dealing with the areas of uncertainty in relation to the definition of “personal information” discussed above:
- the definition in the Act could be amended;
  - the Privacy Commissioner could provide official guidance on the definition; and
  - the resolution of areas of uncertainty could be left to Commissioner case notes and decisions of the Tribunal and the courts.
- 3.28 There is room for each of these options to be used for different issues. Some matters can probably be clarified by amending the definition. These may be matters on which there is already a consensus in opinions of the Commissioner and decisions of the Tribunal and courts, but this does not mean that it is not worthwhile. For one thing, it would put matters beyond doubt, and help to avoid the generally-understood position being overturned in the courts. There is also value in the Act being as explicit as possible, since it has to be applied by countless

---

166 See for example Wendy David “Court: IP Addresses are not ‘Personally Identifiable’ Information” (6 July 2009) [www.mediapost.com](http://www.mediapost.com) (accessed 29 July 2009); “IP Address Alone May Not Be ‘Personal Data’” (summary of a decision of the Hong Kong Privacy Commissioner for Personal Data and subsequent appeal) in Privacy Commissioner for Personal Data *Annual Report 2007–08* (Hong Kong, 2008) 79–81.

167 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 16–17. See also the views of EU Data Protection Supervisor Peter Hustinx: “Hustinx: Nameless Data Can Still be Personal” (6 November 2008) [www.theregister.co.uk](http://www.theregister.co.uk) (accessed 29 July 2009). However, some courts in EU states have held that IP addresses are not personal data, as have some European data protection regulators: Richard Cumbley and Peter Church “EU – What is Personal Data?” *Technology, Media & Telecommunications News* (October 2008) [www.linklaters.com](http://www.linklaters.com) (accessed 30 July 2009); Paul Ohm *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (University of Colorado Law Legal Studies Research Paper No 09–12, 2009) 59.

168 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 308–309.

individuals who do not have the time to familiarise themselves with Privacy Act jurisprudence. Examples of matters that could be made clear in the definition are that “personal information” includes opinions, false information, and information not recorded in a material form. It might also be possible to provide clarification in the statute with regard to identifiability, particularly on the question of the practicality of identification.

- 3.29 Guidance from the Privacy Commissioner could be helpful in clarifying the meaning of “personal information” and assisting agencies to work through whether particular information is covered by the Act or not. Where matters cannot easily be clarified in the statute itself, official guidance from the Commissioner could help to fill some gaps and address specific issues such as IP addresses. It could also use examples, as the guidance from the UK Information Commissioner and the Opinion of the EU Working Party do. However, in addition to the resourcing implications for OPC of developing and consulting on guidelines, there are some potential risks that should be considered. One is that the guidance could be too prescriptive, or could be applied in an overly-mechanical way. It will always be important for the meaning of personal information to be considered in relation to the particular context, and to be applied flexibly so as to be consistent with the spirit and intention of the Act. There is a danger that the guidance could assume more importance than the law itself, and could introduce rule-based regulation by the back door. The other risk is that guidance from the Privacy Commissioner could diverge from authoritative rulings of the courts, as appears to have happened in the UK following the *Durant* decision.
- 3.30 Leaving the meaning of personal information to be clarified through opinions and decisions in particular cases has the advantage of flexibility. There are also some issues (such as the meaning of “about”) that can probably only ever be resolved in relation to the facts of specific cases. However, it takes time for a consensus to develop in the jurisprudence, or for a suitable case to lead to an authoritative court decision. Clarifying the meaning of the Act through jurisprudence is also less accessible to users of the Act than stating matters in legislation or official guidance.
- 3.31 The Law Commission currently believes that the risks of clarifying the definition of “personal information” by means of official guidance from the Privacy Commissioner outweigh the potential benefits. Otherwise, we have no view at present about how the definition should be clarified, and we welcome suggestions.

Q9 Do the following elements of the definition of “personal information” in the Privacy Act need to be clarified? If so, do you have any suggestions about how this should be done?

- “information”
- “about”
- “identifiable”

Q10 Are there any other issues you would like to raise about the definition of “personal information”?

## Human tissue samples and personal information

- 3.32 There is no reference to human tissue or bodily samples in the Privacy Act, but the definition of “health information” in the Health Information Privacy Code 1994 (HIPC) includes:<sup>169</sup>

information provided by [an identifiable] individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual.

There are similar provisions in the definition of “health information” in section 22B of the Health Act 1956. It is clear, therefore, that information derived from human tissue falls within the definition of “health information”. Although not specifically referred to in the Act itself, there is no reason to doubt that information derived from human tissue is included in the general definition of “personal information”, so long as the information is about an identifiable individual.

- 3.33 The question of whether human tissue samples themselves can constitute personal information is a quite different matter. It is difficult to see how such samples could be considered to be personal information under the Act as currently worded. The natural and ordinary meaning of “information” does not include bodily tissue. Rather, such tissue is something from which information may be obtained through testing or other means. The use of the word “about” in the definition of personal information may be another clue: we would not normally say “This blood is about Jane”, whereas we do say “This information is about Jane”. Finally, the reference in the HIPC to information “derived from” the testing or examination of a body part or bodily substance suggests that information is something distinct from the tissue itself. The previous Privacy Commissioner appeared to accept that neither the Privacy Act nor the HIPC apply to bodily samples.<sup>170</sup> This interpretation is consistent with the Article 29 Data Protection Working Party Opinion on the concept of personal data, which specifically states that human tissue samples are sources of data but are not themselves data.<sup>171</sup>

- 3.34 If human tissue samples are excluded from the definition of personal information, the question then becomes whether they should be expressly included in the definition. It appears that the only jurisdiction that currently makes express provision for bodily samples in privacy legislation is New South Wales.<sup>172</sup> The definition of “personal information” in the Privacy and Personal Information

---

169 Health Information Privacy Code 1994, cl 4(1)(d).

170 “Guthrie Tests” (a report by the Privacy Commissioner following his inquiry into the collection, retention, use and release of newborn metabolic screening test samples, September 2003) 8 (para 6.4).

171 Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 9.

172 An expert on international data protection law, Lee Bygrave, believes the NSW provision to be unique: Lee Bygrave “The Body as Data? Reflections on the Relationship of Data Privacy Law with the Human Body” (speech to international conference on “The Body as Data” organised by the Victorian Privacy Commissioner, Melbourne, 8 September 2003) 3.

Act 1998 (NSW) states that the definition “includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics”.<sup>173</sup> According to Privacy NSW, this provision was included in the Act because:<sup>174</sup>

the former Privacy Committee was acutely aware of concerns regarding a number of issues involving bodily samples in the NSW context, for instance, the non-consensual access to and disclosure of newborn screening cards for forensic testing and law enforcement purposes.

3.35 Bodily samples are not expressly covered by the Privacy Act 1988 (Cth), but the ALRC and the Australian Health Ethics Committee (AHEC) recommended in a 2003 report on the protection of human genetic information that the Act should be amended to include bodily samples of identifiable individuals in the definitions of “personal information” and “health information”.<sup>175</sup> This recommendation was rejected by the Australian Government.<sup>176</sup> The key points in the ALRC/AHEC report’s argument for bringing bodily samples within the coverage of the Privacy Act were that:<sup>177</sup>

- Bodily samples are closely analogous to other immediate sources of personal information (such as paper or computer records) that are covered by the privacy principles.
- There are significant gaps in the existing legal protections of the privacy of individuals from whom genetic samples are taken.
- These gaps could be filled by applying the privacy principles to bodily samples, and thereby bringing them within the coverage of an established and well-developed regulatory framework.
- No circumstances had been identified in which adverse consequences for existing practices with regard to the collection and handling of bodily samples could result from the proposed change (although it was acknowledged that special provisions would be needed in the Privacy Act to deal with the application of the privacy principles to bodily samples).

3.36 The argument that, while bodily samples are not themselves information, they are “such an immediate source of personal information (a ‘virtual medical record’) that they demand similar comprehensive privacy protection”,<sup>178</sup> is a strong one. Technology has advanced to the level where genetic testing of human tissue samples can be conducted quickly and increasingly cheaply, and can reveal a significant amount of very personal information about individuals. Furthermore, human tissue samples will often be associated with information that clearly does fall within the definition of personal information in the Privacy Act. For example,

173 Privacy and Personal Information Act 1998 (NSW), s 4(2). This definition is also included in the Health Records and Information Privacy Act 2002 (NSW), s 5(2).

174 Privacy NSW “Supplementary Submission to the Australian Law Reform Commission/Australian Health Ethics Committee Joint Inquiry into the Protection of Human Genetic Information” (December 2002).

175 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 286 (rec 8–2).

176 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 410.

177 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) ch 8.

178 Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 286.

the newborn metabolic screening samples (“Guthrie cards”) clearly fall within the coverage of the Privacy Act and the HIPC because, while the blood spots themselves are not information, the cards contain personal details relating to the baby, the mother and the lead maternity carer.<sup>179</sup> It could, therefore, be considered to be increasingly artificial to separate the treatment of bodily samples from the treatment of the information derived from them.

3.37 However, while it would clearly be undesirable from a privacy perspective if the collection, retention, use and transfer of human tissue samples were unregulated, the Privacy Act is not necessarily the most appropriate vehicle for such regulation. There is already a considerable body of law governing human tissue, including:

- the tort of trespass to the person and the offence of assault<sup>180</sup> (which protect against the non-consensual taking of samples directly from a person);
- the New Zealand Bill of Rights Act 1990;<sup>181</sup>
- the Human Tissue Act 2008 and regulations made under the Act;
- the Health and Disability Commissioner Act 1994, and the Code of Health and Disability Services Consumers’ Rights;<sup>182</sup>
- the Criminal Investigations (Bodily Samples) Act 1995; and
- the Coroners Act 2006.<sup>183</sup>

The Health Act 1956 (section 121A) also makes provision for the making of regulations about the retention of health information and specimens (defined as “bodily sample[s] or tissue sample[s] taken from a person”), although the Health (Retention of Health Information) Regulations 1996 have not been extended to cover specimens so far. In addition, human tissue is governed by research ethics guidelines and requirements for research to be approved by ethics committees.<sup>184</sup>

3.38 This body of law appears to cover at least some of the gaps identified by the ALRC and AHEC in Australia. For example, the Human Tissue Act 2008 specifically provides for the making of regulations with regard to the export and import of human tissue.<sup>185</sup> Moreover, it is difficult to see what benefit there could be in adding the Privacy Act to the already-complex body of law governing

---

179 “Guthrie Tests” (a report by the Privacy Commissioner following his inquiry into the collection, retention, use and release of newborn metabolic screening test samples, September 2003) 3–4. The cards are separated into two parts after they are received at the National Testing Centre. The part that includes the blood spots has only the baby’s surname and National Health Index number written on it, but this part of the card also has a bar code which links it to the other half of the card, containing further personal information about the baby, mother and lead maternity carer.

180 Crimes Act 1961, s 196 (common assault).

181 New Zealand Bill of Rights Act, ss 10 (right not to be subject to medical or scientific experimentation), 11 (right to refuse medical treatment), 21 (right to protection against unreasonable search and seizure).

182 See especially the Code of Health and Disability Services Consumers’ Rights, rights 7(9) and (10).

183 Coroners Act 2006, ss 47–56.

184 See Ministry of Health *Guidelines for the Use of Human Tissue for Future Unspecified Research Purposes* (Wellington, 2007).

185 Human Tissue Act 2008, ss 66, 75. See Australian Law Reform Commission and Australian Health Ethics Committee *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC R96, Sydney, 2003) 271–272 for discussion of this issue in the Australian context.

human tissue samples. While there may be gaps in the existing law,<sup>186</sup> any such gaps are probably best addressed by amending the other statutes and regulations listed above, rather than by extending the scope of the Privacy Act. Amending the definition of “personal information” to include bodily samples would take the privacy principles beyond the area of informational privacy into bodily privacy. This would be a significant expansion, and should not be undertaken lightly, especially given the body of existing law governing human tissue samples. It is probably more appropriate to continue to restrict the coverage of the privacy principles to information derived from such samples. It should also be noted that there is no restriction on the Privacy Commissioner reporting or commenting on matters relating to human tissue samples or other issues of bodily privacy, although this would change if the Commissioner’s functions were to be restricted to informational privacy (see chapter 6). For example, in reports and submissions on the Guthrie cards and on the Criminal Investigations (Bodily Samples) Amendment Bill, the Commissioner has been free to comment on issues regarding the samples themselves as well as associated personal information.

- 3.39 We propose that there should be no change to the current position with regard to human tissue samples and the definition of personal information. If such samples were to be brought within the coverage of the privacy principles, further consultation and analysis would be needed to decide what other changes would be required to the Act.

Q11 Do you agree that human tissue samples should not be covered by the definition of personal information in the Privacy Act? Why, or why not?

Q12 Is any clarification needed with regard to the coverage by the privacy principles of genetic information or other information derived from bodily samples?

“INDIVIDUAL” 3.40 As mentioned above, personal information is defined in the Privacy Act as “information about an identifiable individual”. “Individual” is defined as “a natural person, other than a deceased natural person”. Thus, the definition of individual excludes artificial legal persons (such as companies) or other collective entities, and deceased persons (with some exceptions, discussed below), and consequently information about such persons is excluded from the definition of personal information. The question is whether these exclusions should continue in their current form, be modified, or be removed.

- 3.41 In considering this question, it is important to note that the answer with respect to the Privacy Act need not be the same as with respect to the tort.<sup>187</sup> There are several reasons for this:

186 See Katie Elkin “The New Regulation of Non-Consensual Genetic Analysis in New Zealand” (2008) 16 JLM 246.

187 The application of the privacy tort to corporations and deceased persons is discussed in New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, Wellington, 2009) 152–154; New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, Wellington, 2010) 117–118.

- While the privacy tort is commonly said to protect human dignity, the Privacy Act clearly protects a wider range of interests, including financial interests.
- The Privacy Act protects a broad category of “personal information”, rather than the narrower category of “information in respect of which there is a reasonable expectation of privacy” protected by the tort.
- The Privacy Act has greater scope than the tort for partial or modified application to collective entities and deceased persons, such as applying only some privacy principles to them, applying certain principles only to particular sectors by means of a code, or applying the principles to deceased persons only for a specified period of time after death.

Thus, any decision to include collective entities or deceased persons in the coverage of the Privacy Act should not necessarily influence decisions about the application of the privacy tort, or vice versa.

- 3.42 Any change to the definition of “individual” would affect the Broadcasting Act, which defines “individual” as having the same meaning as in the Privacy Act.<sup>188</sup>

### Deceased persons

- 3.43 While deceased persons are generally excluded from the coverage of the Privacy Act, there are three ways in which information about the deceased does come within the scope of the Act. First, the definition of “personal information” includes “information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act”. Secondly, an agency may refuse to disclose information requested pursuant to principle 6 if the disclosure “would involve the unwarranted disclosure of the affairs of another individual *or of a deceased individual*”.<sup>189</sup> Thirdly, the Act provides that, for the purposes of the issuing of codes of practice relating to health information, principle 11 (disclosure) shall be read as if it applies in respect of any individual, whether living or deceased.<sup>190</sup> Accordingly, the HIPC provides that rule 11 of the Code applies to health information about the deceased for a period of 20 years after death.<sup>191</sup>

### *Existing provisions relating to deceased persons in the Privacy Act*

- 3.44 Several people with extensive knowledge and experience of the Privacy Act have told the Law Commission that the Act needs to be more consistent in its application to deceased persons.<sup>192</sup> The first question, therefore, is whether the existing exceptions to the general rule that the Act does not apply to the deceased are appropriate.

188 Broadcasting Act 1989, s 2(1).

189 Privacy Act 1993, s 29(1)(a) (emphasis added).

190 Privacy Act 1993, s 46(6).

191 Health Information Privacy Code 1994, rule 11(5) and (6). However, health information regarding the deceased may be disclosed if the disclosure is to, or is authorised by, the deceased individual’s representative; or if the information concerns only the fact of death and the disclosure is by a health practitioner or other authorised person to the deceased person’s representative or certain other specified persons: rule 11(1)(a), (b) and (f).

192 Law Commission meeting with people with specialist knowledge of the Privacy Act, 8 May 2008.

## Deaths register

- 3.45 It appears that information about a death maintained pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRRA) was included in the definition of personal information in order to ensure that this information was covered by the public register and information matching controls in the Privacy Act.<sup>193</sup> However, there is no available information about why it was considered desirable that information on the death register should be covered by these controls. It is notable that no similar provision applies to the registers of burials and cremations maintained by local authorities under the Burial and Cremation Act 1964, even though these registers contain names, birth dates and death dates. Information in the burials and cremations registers is not covered by the Privacy Act because it relates to deceased individuals.<sup>194</sup>
- 3.46 Information from the Department of Internal Affairs suggests that the main reasons for extending privacy protection to the deaths register (using the term “deaths register” loosely to include all the various forms in which the Registrar-General maintains information about deaths under the BDMRRA) are that:<sup>195</sup>
- the deaths register includes information about persons other than the individual who has died, and some of these individuals may still be living;<sup>196</sup>
  - the cause of death is recorded on the register, and there may be particular sensitivities in relation to this (for example, if the death was due to suicide or a socially-embarrassing disease); and
  - there is a danger that information from the deaths register may be used to engage in identity crime.
- 3.47 With regard to the first of these points, any information about living individuals contained in the deaths register would be covered by the definition of “personal information” regardless of the specific provision relating to information about a death maintained pursuant to the BDMRRA. This is a good reason for applying privacy protections to the register, but not for including information about deceased persons themselves in the definition of personal information. The second point has some validity, especially given that information about the cause of death will commonly be health information that would be protected against disclosure for 20 years after death under the Health Information Privacy Code. The third point is also persuasive to some extent, although the Department of Internal Affairs acknowledges that restricting access to the BDM register will only go some way towards dealing with the problem of identity crime.<sup>197</sup>

---

193 *Necessary and Desirable* 49.

194 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008) 27–28.

195 Department of Internal Affairs “Review of Public Access to Registers Held in the Citizenship Office and Registry of Birth, Death, and Marriages” (May 2005) paras 26–27, 32–34, 38, 119; Law Commission meeting with Department of Internal Affairs regarding the Births, Deaths, Marriages and Relationships Registration Amendment Bill, 5 March 2007.

196 The Births, Deaths, Marriages, and Relationships Registration (Prescribed Information) Regulations 1995, reg 7, provides that death certificates shall contain information about the deceased’s parents, partners, children, and the doctor who certified the death.

197 Department of Internal Affairs “Review of Public Access to Registers Held in the Citizenship Office and Registry of Birth, Death, and Marriages” (May 2005) para 33.

- 3.48 However, while there may be good reasons to apply some controls to the handling of information on the deaths register, this does not mean that the best way of doing so is to include information about deaths maintained under the BDMRRA in the definition of personal information in the Privacy Act. There are a range of controls on information held on the deaths register in the BDMRRA itself, and this would seem to be the most appropriate way of providing appropriately-targeted protection for information about deceased persons contained in the deaths register. If the Privacy Act were no longer to apply to information about deaths held on the deaths register, some amendments to the BDMRRA might be required.
- 3.49 The question of controls on information matching involving the deaths register is more complex.<sup>198</sup> Section 78A of the BDMRRA authorises the disclosure of deaths information (as well as other information governed by the Act) to certain specified agencies for specified purposes.<sup>199</sup> As at 30 June 2009, eight authorised information-matching programmes involving BDM deaths information were operating.<sup>200</sup> The purposes for which the information is used include detecting benefit fraud, discontinuing benefits to deceased persons, detecting fraudulent passport applications, and cancelling driver licence records relating to deceased persons.<sup>201</sup>
- 3.50 A deceased person cannot be affected by “adverse action” such as discontinuing benefits, but information-matching programmes involving deaths information could affect living persons if the programme results in a false match.<sup>202</sup> Because of the possible impact on living persons, we believe that data matching involving information from the deaths register should continue to be covered by the information-matching provisions of the Privacy Act.
- 3.51 We note that information from the deaths register is sometimes matched with information held by agencies in the private sector. For example, the New Zealand Marketing Association has an agreement with the Department of Internal Affairs which permits information from the deaths index to be used in order to remove deceased persons from mailing lists.<sup>203</sup> The information matching provisions of the Privacy Act do not cover information matching between the public and

198 See also the general discussion of information matching in chapter 9.

199 The specified agencies and purposes are listed in Schedule 1A to the BDMRRA. Information matching involving deaths information is subject to the Registrar-General entering into an agreement with the chief executive of the specified agency; the agreement being limited to a purpose listed in Schedule 1A; and the agreement being an information-matching agreement that complies with the Privacy Act. See Department of Internal Affairs “Identity Services Privacy Notice” [www.dia.govt.nz](http://www.dia.govt.nz) (accessed 15 January 2010).

200 Office of the Privacy Commissioner “List of Statutes and Authorised Information Matching Programmes in Operation” (as at 30 June 2009) on “Data Matching – Operating Programmes” page of the OPC website [www.privacy.org.nz](http://www.privacy.org.nz) (accessed 15 January 2010). In addition, disclosure by the Registrar-General of deaths information is authorised by certain other statutes, most notably the Electoral Act 1993: Department of Internal Affairs “Identity Services Privacy Notice” [www.dia.govt.nz](http://www.dia.govt.nz) (accessed 15 January 2010).

201 The information matching programmes involving BDM deaths information are described in *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2009* (Office of the Privacy Commissioner, Wellington, 2009) 50, 54–55, 65, 66–68, 79–80.

202 For example, between 2004 and 2008 there were 17 challenges to notices of adverse action under the Ministry of Social Development’s deceased persons data-matching programme, and seven of these challenges were successful: *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2008* (Office of the Privacy Commissioner, Wellington, 2008) 56. There were no challenges under this programme in 2008/09.

203 New Zealand Marketing Association “Launching the Upgrade of the Do Not Mail/Do Not Call Service” (June 2009) [www.marketing.org.nz](http://www.marketing.org.nz) (accessed 15 January 2010).

private sectors. Therefore, if the definition of personal information were no longer to include information on the deaths register, use of such information by the private sector would be governed solely by the provisions of the BDMRRA.

- 3.52 Our proposals concerning the Privacy Act and information about deaths maintained by the Registrar-General pursuant to the BDMRRA are as follows:
- consultation should be undertaken with the Department of Internal Affairs and the Registrar-General to determine what amendments, if any, might be required to the BDMRRA if the Privacy Act's coverage of deaths information were to end;
  - the existing provision in the definition of "personal information" should be deleted, subject to any necessary amendments to the BDMRRA being enacted, meaning that for most purposes information about deceased persons on the deaths register will not be covered by the Privacy Act;
  - specific provision should be made in the Privacy Act (or a new Data Matching Act, as proposed in chapter 9) for the application of the information-matching section of the Act to deaths information.

#### Ground for refusal of access

- 3.53 The provision in section 29(1)(a) of the Privacy Act, which allows an agency to refuse access to information requested under principle 6 if it would involve the unwarranted disclosure of the affairs of another individual, whether living or deceased, is based on grounds under the OIA and the Local Government Official Information and Meetings Act 1987.<sup>204</sup> Chapter 11 raises the question of whether there should be greater consistency between the privacy terminology in the OIA and the Privacy Act, and this includes the question of whether the withholding ground in section 9(2)(a) of the OIA should continue to protect the privacy of the deceased. However, even if the OIA withholding ground continues to refer to the privacy of deceased persons, there could be a case for removing or narrowing the reference to deceased persons in section 29(1)(a) of the Privacy Act. The scope of OIA requests is potentially much wider than that of Privacy Act access requests, with greater potential to reveal information about deceased persons that they and their families might reasonably have expected would not be made public. It is also arguable that people's right of access to information about themselves is stronger than their right of access to official information, and furthermore that any information about deceased persons released in response to an access request must, in some sense, also be information relating to the requester.
- 3.54 There do not appear to be any Privacy Commissioner case notes or Tribunal cases that consider the application of section 29(1)(a) to deceased persons. There have been a number of Ombudsmen decisions concerning whether information about deceased persons should be withheld under section 9(2)(a) of the OIA.<sup>205</sup> These decisions, made in consultation with the Privacy Commissioner, seem to

204 Official Information Act 1982, ss 9(2)(a), 27(1)(b); Local Government Official Information and Meetings Act 1987, ss 7(2)(a), 26(1)(b).

205 See for example Case W31776 in 11<sup>th</sup> *Compendium of Case Notes of the Ombudsmen* (Butterworths, Wellington, 1998) 95; Cases A6553, A6580, A6722, W41406, W42031 in 12<sup>th</sup> *Compendium of Case Notes of the Ombudsmen* (Office of the Ombudsmen, Wellington, 2000) 89–95, 97–99.

depend very much on the particular facts of the case. It is noticeable in the OIA cases that the requesters were specifically seeking information about the deceased persons in question, rather than seeking a wider body of information of which the deceased person's information simply formed part. In most cases, the requesters were family members of the deceased person. The Ombudsmen's Practice Guidelines for Official Information provide little guidance about the withholding of information on deceased persons.<sup>206</sup>

- 3.55 We believe that the protection of information relating to deceased persons in section 29 of the Privacy Act is too broad, and should be more consistent with the protection in the rest of the Act. We propose that:
- the words “or of a deceased individual” should be deleted in section 29(1)(a); and
  - a new withholding ground should be added to section 29, dealing with situations where the disclosure of the information would involve the disclosure of health information about a deceased person.<sup>207</sup>
- 3.56 We suggest that the new withholding ground should be broadly consistent with the restrictions on disclosure of health information about deceased persons in rule 11 of the HIPC. That is, it should apply to “health information” as defined in the HIPC for up to 20 years after death, and access should be allowed if the person making the request is the deceased's personal representative or is authorised by the deceased's personal representative. However, in contrast to the HIPC, the withholding ground should not be limited to health information held by a “health agency”.
- 3.57 If any additional protections for information relating to deceased individuals, such as a broader power for the Privacy Commissioner to make provision for information about deceased persons in codes of practice (see below), were to be included in the Privacy Act, further targeted withholding grounds might be needed.

### Health information

- 3.58 Section 46(6) of the Privacy Act, which provides for the application of the disclosure principle to deceased persons for the purposes of any privacy code of practice relating to health information, was introduced by the select committee considering the Privacy of Information Bill. The select committee decided that it was necessary to provide some protection for the medical records of deceased persons, given the sensitive nature of such records and the fact that medical confidentiality has traditionally extended beyond a patient's death.<sup>208</sup>
- 3.59 This provision, and the provisions relating to disclosure of health information about deceased persons in the HIPC, seem to us to be appropriate means of providing protection for information about deceased individuals in the health

---

206 Office of the Ombudsmen *Practice Guidelines: Official Information* available at [www.ombudsmen.govt.nz](http://www.ombudsmen.govt.nz) – see Part B, ch 4.1, 5, and Part E, 4, for brief references to information about deceased persons.

207 One overseas statute (albeit a freedom of information rather than an information privacy statute) that has a specific withholding ground for a deceased person's health information is the Freedom of Information (Scotland) Act 2002, s 38(1)(d).

208 *Necessary and Desirable* 210.

context. We propose below that the Privacy Commissioner’s power to apply codes of practice to information about deceased individuals should be extended. If the Commissioner does not get a general power to make codes covering information about the deceased, however, consideration should be given to the Privacy Commissioner’s recommendations for specific amendments to section 46(6).<sup>209</sup>

Q13 Should there be any changes to the existing provisions relating to deceased persons in the Privacy Act? (See in particular the proposals in paragraphs 3.52 and 3.55.)

#### *Possible new provisions*

- 3.60 The discussion above concerns the existing provisions of the Privacy Act in relation to deceased individuals. We now consider whether any additional provisions in relation to information about deceased individuals are needed. A number of information privacy statutes in Australian states and territories cover personal information about individuals who have been dead for not more than specified periods of time (the longest of which is 30 years).<sup>210</sup> The ALRC has recommended that the Privacy Act 1988 (Cth) should be amended to include specific provisions dealing with the personal information of individuals who have been dead for 30 years or less, where the information is held by an “organisation” (that is, by a private sector body). These provisions should relate to the use and disclosure, access, data quality and data security principles under the Act.<sup>211</sup> The Australian Government has rejected this recommendation, although its main reason for doing so appears to be that there are constitutional limitations on the Federal Government’s power to legislate in this area.<sup>212</sup>
- 3.61 Arguments for extending the Privacy Act’s coverage of information about deceased individuals include:
- People may be reluctant to provide agencies with their personal information while they are alive if they believe that it can be disclosed immediately after their deaths.
  - The families of deceased individuals have an interest in how such individuals’ personal information is handled. They can suffer distress if intimate information about their deceased relatives is disclosed.
  - The idea that deceased persons have no privacy interest may be specific to Pākehā culture, and may not be shared by other cultures.
  - Duties of confidence, which overlap with privacy, can survive death.
  - Some statutes recognise privacy interests of deceased persons, as discussed further below.

209 *Necessary and Desirable* 210–211, rec 75; *1st supplement to Necessary and Desirable* 13–14, rec 75A.

210 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 359–360.

211 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 8–1 and ch 8 generally. The ALRC recommended that information about deceased individuals held by “agencies” (public sector bodies) should continue to be regulated by the Freedom of Information Act 1982 (Cth) and the Archives Act 1983 (Cth): *ibid*, 369.

212 Australian Government *Enhancing Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108 “For Your Information: Australian Privacy Law and Practice”* (Canberra, 2009) 28.

3.62 Arguments against include:

- Privacy is a human right which is inherently personal, and therefore the right of privacy dies with the person.
- The deceased cannot suffer humiliation, loss of dignity, financial loss, threats to physical safety, or any of the other harms that privacy law is intended to protect against.
- The tort of defamation, which is closely related to privacy, does not survive death.
- Applying the Privacy Act to information about deceased persons would be fraught with practical difficulties. In particular, it would be difficult to apply the concept of consent, and to decide how the right of access under principle 6 would apply.

3.63 There is little information available about public attitudes to protection of personal information about deceased individuals. However, a survey conducted for Statistics New Zealand in 2005 found that 26 per cent of respondents would be concerned if all census forms were to be stored with names and addresses attached and then released after 100 years to statistical researchers only. Thirteen per cent of respondents would be “very concerned” (10 on a scale of 0 to 10).<sup>213</sup> Although the majority of respondents were not concerned, it is notable that such a significant minority objected to the release of their information even though they would almost certainly be dead and even if it was to be used only for statistical research. Different cultural perspectives also need to be taken into account. In particular, there is some evidence that Māori beliefs may recognise a right to protection of deceased individuals’ privacy and reputation.<sup>214</sup>

3.64 Some other statutes already recognise the privacy of information about deceased persons to some degree. The explicit reference to the privacy of deceased persons in the OIA has already been mentioned.<sup>215</sup> The Coroners Act 2006 also provides (based on a recommendation by the Law Commission) for coroners to prohibit publication of evidence or submissions to protect “personal privacy”.<sup>216</sup> This does not expressly include the privacy of deceased persons, but nor does it exclude it.<sup>217</sup> The New Zealand Public Health and Disability Act 2000 includes restrictions on the disclosure by mortality review committees appointed under the Act of information that became known to a person only because of the committee’s functions being carried out, along with penalties for breach of these

---

213 *Public Attitudes to the Confidentiality, Privacy and Security of Official Government Survey Data* (survey conducted by UMR Research for Statistics New Zealand, May 2005) 86. The survey was of a nationally-representative sample of 1000 New Zealanders aged 18 and older.

214 Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/BSA, Wellington, 2004) 57; Carol Archie *Pou Kōrero: A Journalists’ Guide to Māori and Current Affairs* (New Zealand Journalists Training Organisation, Wellington, 2007) 87; *Turia v TVNZ* (9 November 2000) Broadcasting Standards Authority 2000–165.

215 Official Information Act 1982, s 9(2)(a).

216 Coroners Act 2006, s 74; New Zealand Law Commission *Coroners* (NZLC R62, Wellington, 2000) 123–124

217 In *Re an inquest into the death of JRF Fardell* (1 November 2006) HC AK CIV 2006-404-3638, para 59, Heath J ruled that “the privacy interests of the deceased and his family” justified a limited suppression order. Although the Coroners Act 2006 was not yet in force, Heath J commented (para 65) that his views on the nature of the discretion to withhold information under the 1988 Act would be equally applicable to section 74 of the new Act.

restrictions.<sup>218</sup> The information handled by mortality review committees will mainly be information about deceased persons, and it is clear that the intention is that such information should be treated as strictly confidential.<sup>219</sup>

### Options for recognising privacy of information about deceased persons

- 3.65 If it is considered desirable to make additional provision in the Act for information about the deceased, there are a number of ways in which this could be done:
- amending the definition of “individual” so that the Privacy Act as a whole applies to information about deceased persons for a specified period after death;
  - introducing a new part of the Act making specific provision for the ways in which some of the privacy principles should apply to information about deceased persons;
  - providing that codes of practice made under the Act can apply to deceased persons; and
  - introducing targeted provisions to deal with specific issues concerning information relating to deceased individuals.
- 3.66 The first option, applying the Privacy Act as a whole to information about deceased persons for a specified period after death, seems too sweeping. There would be major problems about how to apply the privacy principles to information about deceased persons, and amendments to the privacy principles would undoubtedly be required. The second option, which is essentially what the ALRC has recommended, is better. It would mean that only some principles could be applied to deceased persons’ information, and that specific provision could be made as to how these principles would apply. Even so, it would be difficult to come up with provisions that would be suitable for all contexts. New Zealand’s Privacy Act has the advantage of making provision for the creation of codes of practice to deal with the application of the Act to particular sectors. We consider that this would provide greater flexibility and scope to tailor provisions relating to deceased persons to particular contexts.

### Codes of practice

- 3.67 At present, section 46(6) makes very limited provision for the application of a code of practice to information about deceased persons. Section 46(6) deals only with codes of practice relating to health information, and only with principle 11 (disclosure). Disclosure of health information about the deceased is, indeed, a sensitive matter, and it seems appropriate that it should be regulated for 20 years after death. However, other principles may also be applicable to deceased persons’ health information. For example, the Privacy Commissioner has recommended

218 New Zealand Public Health and Disability Act 2000, s 18(7); sch 5, cls 3–6.

219 Perinatal and Maternal Mortality Review Committee “About Us: Privacy of PMMRC Information” [www.pmmrc.health.govt.nz](http://www.pmmrc.health.govt.nz) (accessed 9 September 2009); Child and Youth Mortality Review Committee “About Us: Privacy of CYMRC Information” [www.cymrc.health.govt.nz](http://www.cymrc.health.govt.nz) (accessed 9 September 2009). However, the relevant provisions in the Act are limited to information that is personal information within the meaning of section 2(1) of the Privacy Act: New Zealand Public Health and Disability Act 2000, sch 5, cl 3(a). This means that the provisions do not in fact apply to information about deceased persons except for information about deaths contained in the deaths register.

that principle 5 (security) should apply to such information.<sup>220</sup> Furthermore, there may be contexts other than the health sector in which it would be appropriate to make provision for information relating to deceased persons. One example could be the banking sector. In a letter to the Law Commission, the New Zealand Bankers' Association raised the issue of disclosure of information about deceased customers' accounts. They noted that bankers' common law duty of confidentiality probably continues after death, and that:<sup>221</sup>

Front line staff often experience pressure from relatives of deceased people to provide information about the deceased person's accounts. Some banks consider it appropriate to deal only with the executors of the estates to avoid disputes. Bank staff come under a lot of pressure to disclose information to relatives so clarifying the law in this area would be beneficial.

The Australian Bankers' Association similarly submitted to the ALRC that, as far as possible, banks handle the personal information of deceased individuals in the same way as that of living individuals, and that both should be regulated in the same way.<sup>222</sup> Banking would seem, therefore, to be an industry in which it might be appropriate to extend the coverage of the privacy principles to information about deceased persons by means of a code of practice.

- 3.68 There seems to be no good reason why the application of codes of practice to information about the deceased should be limited to disclosure of health information. There would seem to be a good case for allowing the Privacy Commissioner to apply any of the principles to information about deceased persons in any code of practice that she develops. To be clear, we do not have in mind a generic code of practice relating to information about the deceased. Rather, we propose that codes of practice dealing with particular sectors should be able to apply the principles to information about deceased persons, as the HIPC already does with respect to disclosure of health information.
- 3.69 It could be objected that this gives the Commissioner the power to amend the application of the Act in a very significant way. However, the Act already contains a number of procedural safeguards in relation to codes of practice, and we are proposing to add the additional safeguard of approval by Cabinet. We do not believe that the Commissioner would lightly take the step of applying the principles to information about the deceased, or that such a significant step would fail to be fully debated at several stages in the process.
- 3.70 Our preliminary view is that the Act should be amended to allow codes of practice to be applied to information about deceased persons. We are not inclined to extend the Act's coverage of information about the deceased in any other way.

---

220 *1st supplement to Necessary and Desirable*, rec 75A.

221 New Zealand Bankers' Association to the Law Commission (21 July 2008) Letter.

222 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 366.

Q14 We propose that the Privacy Act should be amended to allow codes of practice to apply any of the privacy principles to information about deceased persons. Do you agree?

Q15 Should any other amendments be made to the Privacy Act to extend its application to information about deceased persons?

### *Survival of Privacy Act complaints after death*

3.71 Another question concerns complaints made by a person who dies before the complaints process has been completed. This issue arose in the case of *Yakas v Kaipara District Council*. In that case, the complainant died after the Privacy Commissioner's investigation had been completed, but before proceedings could be continued in the Tribunal. The complainant's son sought to continue proceedings on his mother's behalf, claiming that the notice of intention to bring proceedings was signed by his mother before her death. There was some uncertainty, however, about when the notice was in fact signed, and the Tribunal had no evidence that the complainant's son was the legal administrator of his mother's estate. The Tribunal did not accept that proceedings could be considered to have commenced while the complainant was still alive. It accepted the defendant's submission that, as the plaintiff was not alive when the claim was commenced, the claim was not brought by an "aggrieved individual" in terms of section 83 of the Privacy Act, and therefore the Tribunal had no jurisdiction to deal with it. The Tribunal noted that the definition of "individual" in the Act excluded deceased natural persons, and that:<sup>223</sup>

In our view the defendant is right to say that section 83 limits the right to bring proceedings in the Tribunal to "aggrieved individuals" in such a way as to ensure that proceedings are brought by individuals on their own account, and that the right to bring proceedings exists only for those individuals who are alive at the time the proceedings are commenced.

As a result, the Tribunal did not need to consider the defendant's alternative submission, that any cause of action the plaintiff may have had under the Act could not be pursued by her estate after her death.

3.72 Paul Roth has questioned the Tribunal's interpretation of the Act in *Yakas*. The Tribunal seemed to rely not only on the definition of "individual" but also on the provision in section 83 that the aggrieved individual "may himself or herself" bring proceedings before the Tribunal. Roth suggests that, rather than requiring that an individual personally bring proceedings on his or her own account, this provision in section 83 can be seen as standing in contrast to the position in section 82(2), which refers to the bringing of proceedings by the Director of Human Rights Proceedings. If this interpretation is accepted, Roth argues:<sup>224</sup>

then the words no longer suggest that proceedings may only be brought personally by living individuals, but might also be brought on behalf of individuals who were alive when the cause of action under the Privacy Act accrued.

<sup>223</sup> *Yakas v Kaipara District Council* [2004] NZHRRT 10, para 11.

<sup>224</sup> Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA83.4(c), 503,214.

- 3.73 Whatever the correct legal position with regard to the current provisions of the Act and the particular facts of *Yakas*, it seems wrong in principle (as Roth also argues) “that causes of action under the Privacy Act should be barred by death, and that the ‘aggrieved individual’ cannot be represented, after death, by the executor or administrator of his or her estate”.<sup>225</sup> Section 3(1) of the Law Reform Act 1936 provides that, on the death of any person, all causes of action (apart from defamation) vested in the deceased person shall survive for the benefit of his or her estate. In principle, Privacy Act proceedings in the Tribunal under section 83 should be covered by this provision in the Law Reform Act, and if a contrary intention is suggested by the wording of section 83 this should probably be amended. Roth makes the point that, if causes of action under the Privacy Act are rendered void by death, this could create an incentive for respondents to be obstructive so as to delay the Commissioner’s investigations in the hope that the complainant will die before the matter is resolved. Proceedings brought by the Director of Human Rights Proceedings under section 82 (which may in future be brought by the Privacy Commissioner under our proposals in chapter 8) are probably a different matter. Comments by the Court of Appeal in a case relating to the Health and Disability Commissioner Act suggest that a case brought by the Director may not be a “cause of action” in terms of section 3(1) of the Law Reform Act 1936.<sup>226</sup>
- 3.74 The question of what should happen when a complainant dies while a complaint is still at the stage of mediation or investigation by the Privacy Commissioner is perhaps less clear. At this stage, the complaint is probably not a “cause of action” that would be covered by the Law Reform Act 1936. There is probably no reason why the Commissioner cannot continue mediation with the executor or administrator of the deceased’s estate, or with a person or persons nominated by the deceased prior to death to represent him or her, if the respondent agrees. However, if the respondent does not agree to such a process, or if the parties are unable to reach an agreed settlement, it is unclear how the Commissioner should proceed. Certainly, the Commissioner has discretion under section 71(2) of the Act to take no further action if it appears that, “having regard to all the circumstances of the case, any further action is unnecessary or inappropriate”. Normally, where the Commissioner has decided that a complaint ought not to be proceeded with, the complainant has a right under section 83 to bring proceedings before the Tribunal. Does the Commissioner’s decision to take no further action on a complaint give rise to a “cause of action” that can then be pursued by the deceased’s representatives? At what point, precisely, does a cause of action accrue? On the other hand, if the Commissioner considers that further action is appropriate (perhaps because the complaint reveals wider systemic problems), can an investigation be continued despite the complainant’s death?
- 3.75 We propose that the Privacy Act should be amended to make clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act.

---

225 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA83.4(c), 503,214.

226 *Marks v Director of Health and Disability Proceedings* [2009] NZCA 151, para 65 Glazebrook J.

Q16 We propose that the Privacy Act should be amended to make clear that section 3(1) of the Law Reform Act 1936 applies to causes of action under the Privacy Act. Do you agree? Do you have any other suggestions about survival of Privacy Act complaints after death?

### Legal persons and groups

- 3.76 Section 29 of the Interpretation Act 1999 defines “person” as including “a corporation sole, a body corporate, and an unincorporated body”. By consistently using the term “individual” rather than “person”, and by limiting the meaning of “individual” to natural persons, the drafters of the Privacy Act ensured that it would not apply to the handling of information relating to corporations or unincorporated groups. Unlike the exclusion of information about deceased persons, there are currently no exceptions to the exclusion of information about legal persons and other collective entities.
- 3.77 There is limited recognition of the privacy interests of corporations in other legislation. The OIA defines person as including “a corporation sole, and also a body of persons, whether corporate or unincorporated”.<sup>227</sup> Sections 24 to 27 of the OIA provide for rights of access to and correction of official information about an identifiable person. These provisions originally applied to both natural and legal persons, but following the enactment of the Privacy Act the OIA provisions were amended so that they now confer access and correction rights only on bodies corporate.<sup>228</sup> It is also worth noting that section 29 of the New Zealand Bill of Rights Act 1990 provides that the provisions of the Bill of Rights apply, “so far as practicable”, for the benefit of legal persons. This means, among other things, that legal persons can benefit from the protection of privacy in section 21 of the Bill of Rights Act: protection against unreasonable search and seizure.
- 3.78 The OECD Privacy Guidelines, with which the Privacy Act is said to be “in general accordance” (Long Title to the Act), do not deal with information relating to legal persons or groups.<sup>229</sup> They define “personal data” as information relating to an identified or identifiable “individual”.<sup>230</sup> The Expert Group established to develop the Guidelines specifically considered whether the Guidelines should cover legal persons and groups, but no consensus could be reached on this issue. However, the Guidelines only establish minimum standards for domestic legislation, and there is nothing to prevent member countries from developing data protection laws and policies for corporations and groups.<sup>231</sup> Most personal data protection statutes in other jurisdictions apply only to information about natural persons, but a small number of countries also apply data protection

227 Official Information Act 1982, s 2(1).

228 Official Information Act 1982, s 24(2).

229 For a comprehensive, comparative survey of issues relating to data protection rights for private collective entities see Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) chs 9–16.

230 Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), para 1(b).

231 Explanatory Memorandum to the OECD Privacy Guidelines, paras 19(c), 31–33, 49.

laws to information about legal persons, at least to some extent.<sup>232</sup> In line with the recommendation of the South African Law Reform Commission, the Protection of Personal Information Bill recently introduced in South Africa provides that “personal information” can, “where it is applicable”, include information about a “juristic person”.<sup>233</sup> By contrast, the ALRC recommended that the Privacy Act 1988 (Cth) should not be amended to cover information about corporations or groups.<sup>234</sup>

- 3.79 We do not favour extending the Privacy Act to cover corporations. We believe that such an extension is inconsistent with the purpose of the Act, which is “to promote and protect *individual* privacy”<sup>235</sup> in accordance with the OECD Guidelines and with international human rights law. Privacy is a human right, based ultimately on protection of individual dignity, and the harms that can be suffered by corporations through misuse of their information are fundamentally different from those which can be suffered by individuals. The interests of corporations that are akin to privacy are adequately protected by other areas of law, including breach of confidence, defamation, intellectual property, and laws criminalising various forms of surveillance, computer hacking, and theft of information. Furthermore, corporations are inherently public bodies which take on obligations of transparency in return for the protections that come with their legal status. They do not have the same rights as individuals to keep their information private (although, as noted, they can protect some kinds of information through other branches of law). Extending the Privacy Act to cover corporations would also give rise to uncertainty and practical difficulties about the application of the privacy principles, and would add to compliance costs.
- 3.80 While we do not favour giving corporations rights under the Privacy Act, we invite submissions on the specific question of whether corporations should have rights of access or correction under principles 6 and 7. Gehan Gunasekara from the University of Auckland has proposed that, at a minimum, corporations should be given access and correction rights, which would be consistent with the rights that they already possess with respect to official information.<sup>236</sup> There is a danger, however, that if access rights were to be extended to corporations, they could be used by companies to gather intelligence about the information held about them by their competitors. This could include information about their competitors’ attitudes towards them and business strategies for competing with them. This objection would not apply if access and correction rights were limited to the field of credit reporting. Several Scandinavian countries that do not make

---

232 Argentina, Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland have enacted data protection legislation expressly covering legal persons or other collective entities. However, in 2000 Denmark, Iceland and Norway either abolished or reduced the coverage of data relating to legal persons in their data protection laws. Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 178–179, 195; Personal Data Protection Act of 2000 (Argentina), s 2.

233 Protection of Personal Information Bill (South Africa), B 9-2009, cl 1; South African Law Reform Commission *Privacy and Data Protection: Report* (SALRC Project 124, Pretoria, 2009) 72–84.

234 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) ch 7.

235 Long Title to the Privacy Act 1993 (emphasis added).

236 Gehan Gunasekara “Privacy Rights for Companies?” [2008] NZLJ 30.

general provision for information about corporations in their data protection laws do, however, provide for rights of corporations with respect to information held about them by credit reporting companies.<sup>237</sup> Gunasekara argues that:<sup>238</sup>

In a credit-driven economy, accurate credit reporting and the right to verify and correct inaccurate statements are invaluable. Accurate reporting is just as important to companies whose credit-worthiness is their most important asset. It is difficult to see what justification exists to deny companies the same rights as natural persons in this area.

There is at least an arguable case, therefore, for providing in the Act that any code relating to credit reporting may provide for access and correction rights for corporations.

- 3.81 The question of whether the Privacy Act should apply to unincorporated groups is somewhat different from the question of its application to legal persons.<sup>239</sup> The idea of collective privacy or group rights to privacy has been raised, particularly in relation to information about Māori and other indigenous peoples,<sup>240</sup> but it is hard to see how it could work in practice. The Privacy Act is based on each individual's rights to control information relating to that individual, and it is very difficult to see how it could apply to groups without legal personality. Unincorporated bodies, such as sporting clubs or Māori tribes that do not have a legal identity recognised under statute, cannot sue in tort. They may, however, have common interests that the law could recognise. We suggest that the best way of doing so would be by making better provision in the Privacy Act for representative complaints, as discussed in chapter 8.

Q17 Should the Act provide that any code of practice relating to the credit reporting industry may provide for access and correction rights for corporations? Should the Act provide generally for access and correction rights for corporations?

*Can information about a corporation be information about an individual?*

- 3.82 The issue of whether, in some circumstances, information about a corporation can be information about the person or persons behind that corporation, came up in a Complaints Review Tribunal case, *C v ASB Bank*. C was the sole director and owner of all but one share in a business, and he used the company's bank account for personal as well as business transactions. After he and his wife separated, his wife obtained copies of the company's bank statements from the bank.

237 Denmark's data protection law applies to corporations in respect of information held about them by credit reporting agencies; Sweden provides in its Credit Reporting Act for access and correction rights of corporations in relation to information held by credit reporting agencies; and Norway's data protection law allowed (as of 2002) for the future introduction of protection for legal persons with respect to credit reporting information: Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 195, 202, 206.

238 Gehan Gunasekara "Privacy Rights for Companies?" [2008] NZLJ 30, 30.

239 See Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) ch 15.

240 New Zealand Law Commission *Privacy: Concepts and Issues* (NZLC SP19, Wellington, 2008) 106–107; Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) 339–351.

C complained about this unauthorised disclosure by the bank, and submitted to the Tribunal that the bank statements were personal information. He argued that “information which appears on its face to be information about a company rather than an identifiable individual can be transformed into personal information” by factors such as the nature of the company (the fact that it was a one-person operation); the fact that the account was used in part for personal transactions; the purpose for which his wife obtained the information (she was interested in information about him, not about the company); and the use to which the information was put (the fact that it was combined with other information about him held by his wife and used to draw conclusions about him). The Tribunal agreed with the defendant bank’s submission that the information was about the company, not about C, and was therefore outside the scope of the Privacy Act. In the Tribunal’s view, it could not find otherwise without lifting the corporate veil and disregarding a century of company law.<sup>241</sup>

- 3.83 The Tribunal’s very strict interpretation in *C v ASB Bank* seems out of character with the spirit and the generally flexible approach of the Privacy Act.<sup>242</sup> In its 1983 report on privacy, the ALRC stated that:<sup>243</sup>

The creation of a corporate or other business structure for a commercial, family or other purpose should not prevent a claim, in the name of a business association, which is in essence one affecting intimate personal interests of an identifiable private individual. A person should have standing ... where he can show that his claim, while nominally concerning an artificial legal person, would affect his personal interests. In other words, [the Privacy Commissioner should] be entitled to pierce the corporate veil and investigate any complaint which, while in appearance one concerning a corporation, was in reality one concerning an individual.

We believe that this is the preferable approach, and that the Privacy Act should be amended to make this clear. To do otherwise is to leave a gap in the Privacy Act’s coverage of information that, by any reasonable interpretation, relates to an identifiable individual.<sup>244</sup> However, we recognise that, by “piercing the corporate veil”, such a proposal could be seen as “disregard[ing] a hundred years of company law and jurisprudence”.<sup>245</sup> We therefore invite submissions on the implications for other areas of law.

- 3.84 A related question, about which we also seek submissions, concerns the circumstances in which information about a trust can be personal information, and whether the Privacy Act should make provision for information about trusts.

---

241 *C v ASB Bank Ltd* (26 August 1997) Complaints Review Tribunal 21/97.

242 Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 211–212; Paul Roth “What is Personal Information?” (2002) 20 NZULR 40, 57–58.

243 Australian Law Reform Commission *Privacy* (vol 1, ALRC R22, Australian Government Publishing Service, Canberra, 1983) 15.

244 Lee A Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, The Hague, 2002) 210–215; Article 29 Data Protection Working Party *Opinion 4/2007 on the Concept of Personal Data* (WP 136, adopted 20 June 2007) 23–24.

245 *C v ASB Bank Ltd* (26 August 1997) Complaints Review Tribunal 21/97, 4 (quoting the words of counsel for the defendant).

Q18 We propose that the Privacy Act should be amended to make clear that, despite the general exclusion of information about legal persons from the definition of personal information, information about a legal person can be personal information if it is also clearly information about an identifiable individual. Do you agree? Would this have implications for other areas of law?

Q19 Should the Privacy Act be amended to clarify the circumstances in which information about a trust can be personal information?

## "COLLECT"

- 3.85 The definition of "collect" in the Privacy Act states simply that "**Collect** does not include receipt of unsolicited information." The sole purpose of the definition, then, is to provide that unsolicited information will not be "collected" for the purpose of the Act ("the unsolicited information exception"), and therefore will not be covered by the collection principles (principles 1 to 4). The definition of "collect" does not affect the interpretation of the other privacy principles, as principles 5 to 12 do not use the word "collect". Principles 5 to 11 refer to information that an agency "holds", and principles 10 and 11 also refer to the purposes for which information was "obtained". "Obtained" is undefined, but it seems clear that it includes both information that was collected by the agency and information that is held by the agency but was unsolicited. The Act does not define "unsolicited" or "solicit".
- 3.86 A report to the Minister of Justice on the Privacy of Information Bill suggested definitions of "collect" and "obtain", but these were not included in the Bill.<sup>246</sup> The report defined "collect" as including "solicit, and the taking of any other action by the agency to get personal information into its possession from outside the agency", while "obtain" was defined as including "solicit, collect, and the coming into possession of personal information from outside the agency in any other way".
- 3.87 It does not seem to be common internationally to define "collect" in information privacy legislation, or to specifically exclude receipt of unsolicited information from the meaning of "collect". However, the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW) both provide that information is not collected for the purposes of the Acts if receipt of that information is unsolicited.<sup>247</sup> In addition, Information Privacy Principles 2 and 3 in the Privacy Act 1988 (Cth) apply only to information that is solicited by the collector.<sup>248</sup> "Solicit" is defined, in relation to personal information, as meaning "request a person to provide that information, or a kind of information in which that information is included."<sup>249</sup> However, the National

246 *Privacy of Information Bill: Directions Report to the Minister of Justice* (23 October 1992), cited in Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA2.5, 6.13(b), 201,801, 204,201.

247 Privacy and Personal Information Protection Act 1998 (NSW), s 4(5); Health Records and Information Privacy Act 2002 (NSW), s 10.

248 Privacy Act 1988 (Cth), s 14.

249 Privacy Act 1988 (Cth), s 6(1).

Privacy Principles in the same Act do not distinguish between solicited and unsolicited information. The ALRC's proposed Unified Privacy Principle 2 (Collection) would not exclude unsolicited information from its coverage, but would include special provisions about how unsolicited information should be handled. Essentially, the ALRC recommends that unsolicited information should either be destroyed or, if it is retained, treated in the same way as if it had been actively collected.<sup>250</sup>

- 3.88 We propose in chapter 4 that privacy principle 2 should be amended to include a provision about the handling of unsolicited information along the lines of the ALRC's recommendation. This proposal can go ahead regardless of whether or not the unsolicited information exception is retained.
- 3.89 The main difficulty created by the definition of "collect" is the potential for uncertainty about what "unsolicited" means. Some types of information are clearly unsolicited. For example:<sup>251</sup>
- Information about an individual may be provided to an agency by a third party without the agency asking for it (as in the case of a tip-off that a person is engaging in benefit fraud).
  - Information may be sent to an agency by mistake (as in the case of misdirected mail, faxes or emails).
  - Promotional material containing personal information may be sent to an agency without the agency having invited such material (as in the case of a business flyer which includes names and contact details).
- 3.90 While the examples just given are reasonably straightforward, there are a number of ways in which the unsolicited information exception may cause uncertainty about the scope of "collection". In particular, Paul Roth has raised the question of whether surveillance by means of a recording or monitoring device is collection for the purposes of the Act. He argues that such surveillance is not collection because information is not solicited in the sense of a request for information being made to a person. This interpretation is not accepted by either the Privacy Commissioner or the Human Rights Review Tribunal, both of which have consistently taken the view that the use of surveillance to obtain information does constitute collection.<sup>252</sup>
- 3.91 There was limited support for Roth's view in the Court of Appeal decision in *Harder v Proceedings Commissioner*. That case involved two conversations between the complainant and a lawyer, both of which the lawyer recorded without informing the complainant that he was doing so. The first phone call was unsolicited in the sense that it was made by the complainant of her own accord, while the second phone call was solicited in that it had been arranged that the complainant would ring the lawyer back. With respect to the first conversation, the Complaints Review Tribunal concluded that, by switching on the tape recorder, the lawyer had ceased to be a passive recipient of unsolicited

250 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 21-3, 726.

251 Office of the Privacy Commissioner (Federal) *Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72* (Sydney, 2007) 317.

252 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA2.5, 151,802–151,803.

information and had become an active collector of the information. The Court of Appeal disagreed, holding that “The unsolicited nature of the information was not affected by the fact that it was recorded or the way it was recorded. It was therefore not relevantly collected.”<sup>253</sup> It must be emphasised, however, that the question at issue was whether information that was otherwise unsolicited (and therefore not collected) could be transformed into information that was collected by the simple act of recording it. *Harder* is of limited relevance to a situation such as deliberately installing a camera in order to obtain images of people in a particular area.

- 3.92 Surveillance is not the only area in which the meaning of “unsolicited”, and therefore of “collect”, may be unclear. Another example concerns agencies, or sections within agencies, that exist in order to receive inquiries or complaints (for example, customer service or complaints departments within commercial enterprises, or complaints bodies such as professional disciplinary tribunals). Do such agencies “solicit” the information that is provided to them? Paul Roth asks:<sup>254</sup>

Can alerting customers to the existence of such a service, and directing them to it in the case of complaints, mean that the agency concerned is, in a sense, “collecting” such information, or is any information obtained through such channels still “unsolicited”?

This issue has come up in relation to the similar unsolicited information exception in the NSW legislation. In one case, involving disclosure to a doctor who was the subject of a complaint to the NSW Medical Board of information provided as part of that complaint, the Administrative Decisions Tribunal found that the complaint to the Medical Board was unsolicited. The Tribunal commented that “virtually all complaints received by investigative agencies will be unsolicited”, although that did not mean that all information provided by complainants to such agencies will be unsolicited.<sup>255</sup> However, Privacy NSW has said that agencies should not treat complaints to them as unsolicited if they hold themselves out as being the appropriate body to receive such complaints.<sup>256</sup>

- 3.93 A third area of possible uncertainty concerns what could be called “internally-generated information”. Examples include:
- The outcome of a completed disciplinary process. In *Boyle v Manurewa RSA Inc*, the Human Rights Review Tribunal found that the outcome of a disciplinary process that had run its course was not information that had been “collected” for the purposes of the Privacy Act.<sup>257</sup>
  - Information that is generated automatically in the course of a transaction or similar activity. In a submission to the Privacy Commissioner’s *Necessary and Desirable* review, Telecom New Zealand stated that it was unclear whether “collect” included automatically-generated information, such as certain types

253 *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, para 25 (CA) Tipping J.

254 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.5, 151,801.

255 *KD v Registrar, NSW Medical Board* [2004] NSWADT 5, para 27.

256 New South Wales Law Reform Commission *Privacy Legislation in New South Wales* (NSWLRC CP3, Sydney, 2008) 87.

257 *Boyle v Manurewa RSA Inc* [2003] NZHRRT 16, para 31.

of call records about individual subscribers. Telecom considered that the generation of such records should fall within the definition of “collect”, and that the definition could be amended to make this clear.<sup>258</sup>

- Information contained in employee emails archived by the employer’s computer system. Paul Roth comments that:<sup>259</sup>

Personal information extracted from a computer that automatically archives or maintains a record of all e-mail messages would presumably constitute the receipt of unsolicited information, as the personal information disclosed in the messages would not have been solicited from the individual concerned... .

- 3.94 Considering the meanings of “collect”, “solicit” and “unsolicited” in ordinary usage is of some assistance. Dictionary definitions of “collect” include “bring or come together; assemble, accumulate”; “systematically seek and acquire (books, stamps, etc.), esp. as a continuing hobby”; “obtain (taxes, contributions, etc.) from a number of people”; “call for; fetch; obtain or gather (*went to collect the laundry*)”; and “infer, gather, conclude”.<sup>260</sup> These definitions tend to suggest that collection involves making some effort to acquire something, and especially that to collect something is to acquire it or bring specimens of it together systematically or purposefully. The natural and ordinary meaning of “collect” would, therefore, probably include some instances in which material has not been directly requested or invited, but would not include instances in which material is received accidentally, due to a misunderstanding, or without any indication having been given of an interest in receiving the material. For example, if a postage stamp collector is given postage stamps as gifts, and she puts them in her stamp album, she has collected them. Even though she has not directly asked for them, she has made her general interest in stamps known, she has a purpose for keeping them, and she has added them systematically to her existing collection. If, on the other hand, someone misunderstands her interest and gives her a rubber stamp, she would not have collected this stamp even if, through sheer inertia, she never gets around to throwing it away. Even without the express exclusion of unsolicited information, then, the Privacy Commissioner, the Tribunal or the courts may interpret “collect” as excluding some cases of receipt of unsolicited information.<sup>261</sup> The question is whether the exclusion of all unsolicited information from the meaning of “collect” is appropriate.

---

258 Telecom New Zealand, submission on Discussion Paper 1 for Privacy Commissioner Review of the Privacy Act 1993, 23 October 1997.

259 Paul Roth *Privacy Law and Practice* (loose leaf, LexisNexis, Wellington, Privacy Act 1993, 2007) PVA 2.5, 151,805.

260 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (South Melbourne, Oxford University Press, 2005) 214.

261 See *OA v New South Wales Department of Housing* [2005] NSWADT 233, para 36: “The mere receipt of a communication from the member of the public does not constitute a ‘collection’ of personal information, as it does not involve an act on the part of the agency of ‘assembling’ or ‘gathering’ the information (see definitions of ‘collect’ and ‘collection’ in *Macquarie Dictionary*, (1<sup>st</sup> ed, 1980).” The NSW Administrative Decisions Tribunal considered that the express exclusion of unsolicited information in section 4(5) of the Privacy and Personal Information Protection Act 1998 (NSW) simply put the matter beyond doubt.

- 3.95 To “solicit” is to “ask repeatedly or earnestly for or seek or invite” or to “make a request or petition to (a person)”. “Unsolicited” means “not asked for; given or done voluntarily”.<sup>262</sup> “Solicit” clearly has a narrower meaning than “collect”, and would seem to require either a direct request to an individual or some kind of invitation (whether that be to specific people or to the public at large). As noted above, the Privacy Act 1988 (Cth) currently defines “solicit” in terms of requesting someone to provide information. Guidance from the Federal Privacy Commissioner in Australia states that an agency asks for or solicits information if it encourages people or organisations to give it information, including asking directly for information, arranging for information to be provided to it regularly, or encouraging people to give it information by such means as setting up a hotline.<sup>263</sup>
- 3.96 If the term “unsolicited” is considered in isolation, then, there is some sense to the argument that the unsolicited information exception means that certain types of surveillance are excluded from the coverage of the collection principles. Where a CCTV camera sits passively recording images of people it is hard to see how the information obtained can be said to have been solicited from the people who have been recorded by the camera. They are not asked if they want to be filmed, and they may not even be aware that they are being recorded. The unsolicited nature of such surveillance is even more obvious if the camera is hidden. However, if the meaning of “unsolicited” is considered in context as part of the definition of “collect”, matters are less clear. As noted above, “collect” suggests making some effort to acquire information or acquiring it purposefully or systematically. It is probably only information that the agency has made no attempt to acquire that the unsolicited information exception is intended to exclude. The Office of the Privacy Commissioner website states that:<sup>264</sup>

To collect information, the agency must, in some way, ask to get it. This includes setting up equipment to record anything that happens in an area. It is not a “collection” if the agency is just given information that it did not ask for.

The overall purpose of and background to the Act, including the desire to protect people against collection by unlawful, unfair or unreasonably intrusive means (principle 4), suggest that surveillance should be considered a form of collection of information. This is supported by the Explanatory Memorandum to the OECD Privacy Guidelines, which states that the Collection Limitation principle is directed, in part, at such practices as “the use of hidden data registration devices such as tape recorders”.<sup>265</sup> Certainly, if it were not for the unsolicited information exception, there could be little doubt that a CCTV camera is collecting information in the ordinary meaning of the word “collect”.

262 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (South Melbourne, Oxford University Press, 2005) 1073, 1237. See also the definition of “unsolicited” in the Unsolicited Goods and Services Act 1975, s 2(1): “**Unsolicited** means, in relation to goods sent to any person, that they are sent without any prior request made by him or on his behalf.”

263 Office of the Privacy Commissioner (Australia) *Plain English Guidelines to Information Privacy Principles 1–3* (Sydney, 1994) 4.

264 “Glossary” at [www.privacy.org.nz/glossary](http://www.privacy.org.nz/glossary) (accessed 17 September 2009).

265 Explanatory Memorandum to the OECD Privacy Guidelines, para 52.

- 3.97 Information received by complaints bodies as part of a complaint should also probably fall within the definition of “collect” already. Such information is solicited in the sense that it is asked for or invited in a general way by the agency, even if the agency has not specifically requested each individual complaint. Internally-generated information is more ambiguous. Even without the exclusion of unsolicited information, it could be debatable whether a record of the fact that a particular transaction took place or that a particular disciplinary decision was taken constitutes a collection of that fact. In terms of the current definition of “collect”, it is also hard to see how such information can be said to have been “solicited”.
- 3.98 It appears, therefore, that there is at least some room for uncertainty about the meaning of “collect”, and some matters that could be put beyond doubt by amending the definition in some way. There are three options for reforming the definition of “collect”: deleting it, amending it, or clarifying it by means of guidance from the Privacy Commissioner.
- 3.99 The first option would be to remove the express exclusion of receipt of unsolicited information; in other words, to leave “collect” undefined. This would mean abolishing the distinction between solicited and unsolicited information, and should be considered together with our proposal in chapter 4 to adopt the ALRC’s recommendation with regard to the treatment of unsolicited information. This approach would clearly deal with Paul Roth’s point about collection and surveillance. It would, however, leave some continuing uncertainty about the scope of the term “collect”. It is also possible that simply deleting the current definition would be interpreted as an indication that Parliament intends that all forms of unsolicited information should be considered to be collected for the purposes of the Act. We do not think that information which an agency has taken no steps to obtain should be considered to have been collected by that agency, although we do propose in chapter 4 that, if the agency does not destroy the information, it should treat it in the same way as if it had been collected.
- 3.100 The second option would be to revise the definition of “collect”. This, in turn, could be done either by retaining the existing definition but adding a definition of “solicit” or “unsolicited”, or by changing the definition so that it is not based on excluding unsolicited information but instead tries to spell out more clearly what “collect” means. The definition of “collect” in the report to the Minister of Justice on the Privacy of Information Bill, quoted above, is an example of the latter approach. The main problem with this approach is that it could be difficult to come up with a satisfactory definition. One possibility would be to leave the current definition of “collect”, but add to it some specific provisions making clear that certain types of information (such as surveillance information and transaction records) are included in the definition. Another approach would be to define more precisely what is *excluded* from the definition: for example, the definition could exclude information obtained by mistake or sent to the agency without any form of request for the information having been made by the agency.

- 3.101 A third option, which could be combined with one of the first two options, would be for the Privacy Commissioner to develop guidance on these matters. The ALRC has recommended that the Office of the Privacy Commissioner should develop guidance about the meaning of “unsolicited” in the context of the collection principle in the Privacy Act 1988 (Cth).<sup>266</sup>
- 3.102 We propose that the definition of “collect” should simply be deleted, thereby removing the exclusion of receipt of unsolicited information. This would be consistent with the approach in most other jurisdictions and with the ALRC’s proposed approach in Australia, and would remove problems with the current definition, particularly in relation to surveillance. It would be supported by the proposal in chapter 4 that agencies that receive unsolicited information should either destroy it or, if they retain it, treat it in the same way as if it had been actively collected. Other changes to the collection principles proposed in chapter 4 should also be considered in relation to the discussion of the definition of “collect”.

Q20 We propose that the definition of “collect” should be deleted. Do you agree? If not, should it be clarified in some way?

#### OTHER TERMS

- 3.103 Other chapters discuss the definitions of particular terms relevant to those chapters. For example, the definitions of “agency”, “news activity” and “news medium” are discussed in chapter 5. However, there may be other terms used in the Act that are currently undefined but that should be defined; or terms that are currently defined but whose definitions should be amended. For example, the terms “hold” and “obtain” could be defined, or the term “publicly available publication” could be amended to clarify its application to online information.

Q21 Are there any other terms that need to be defined, or whose definitions should be amended?

<sup>266</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) rec 21-4, 726.