16. New Regulatory Mechanisms

Contents

Summary 309
Privacy Commissioner investigations for serious invasions of privacy 310
Deletion, removal and de-identification 312
Complaints about media invasions of privacy 314
Conciliation process 316
Amicus curiae and intervener functions 317
An amicus curiae function for the Commissioner 318
An intervener function for the Commissioner 318
Deletion of personal information 319
Review of the small business exemption 321

Summary

16.1 This chapter sets out recommendations about new regulatory mechanisms to reduce and redress serious invasions of privacy. The new regulatory powers the ALRC recommends in this chapter are not intended to be an alternative to a statutory tort for serious invasions of privacy—although, in the absence of a statutory tort, the new regulatory powers would increase the legal protection of privacy. Rather, the new regulatory powers would complement a statutory tort, providing a low cost alternative to litigation, which may, in some cases, lead to a satisfactory outcome for parties.

16.2 The ALRC recommends that consideration be given to conferring extended powers on the Privacy Commissioner to investigate complaints about serious invasions of privacy. This would provide a forum for consideration of complaints about serious invasions of privacy without requiring parties to commit the time and resources that might be needed for court proceedings. Under these extended powers, the Commissioner could be given the power to recommend the non-publication or removal of private information from publication. However, court action would be required to enforce such a recommendation.

16.3 The ALRC also recommends conferring additional functions on the Privacy Commissioner to act as amicus curiae or intervener in court proceedings, with the leave of the court, where the Commissioner considers it appropriate.

Privacy Commissioner investigations for serious invasions of privacy

Recommendation 16–1 The Commonwealth Government should consider extending the Privacy Commissioner's powers so that the Commissioner may investigate complaints about serious invasions of privacy and make appropriate declarations. Such declarations would require referral to a court for enforcement.

16.4 There may be a number of benefits to empowering the Privacy Commissioner to investigate complaints about serious invasions of privacy, in addition to providing a cause of action allowing individuals to undertake court proceedings for serious invasion of privacy.[1] These benefits may include:

- greater accessibility and lower cost of a complaints mechanism as compared to court proceedings;[2]
- use of the Commissioner's experience and expertise in handling privacy complaints;[3]
- benefits of providing the Commissioner with a formal role in addressing serious invasions of privacy, including the benefits of avoiding the fragmentation that might occur if the Commissioner had no such role;[4] and
- significant public awareness of the Commissioner in relation to privacy concerns.[5]

16.5 The mechanism might face challenges, including:

- the need for additional resources to be provided to the Commissioner; and
- the limitations of exemptions in the *Privacy Act 1988* (Cth), which generally does not apply to individuals, small businesses or media organisations.

16.6 A power for the Commissioner to investigate complaints about serious invasions of privacy could be integrated with the Commissioner's existing powers to investigate

---

1 Under the *Privacy Act 1988* (Cth), privacy functions are conferred on the Australian Information Commissioner. However, in the 2014 Budget, the Australian Government announced an intention to disband the Office of the Australian Information Commissioner. The Privacy Commissioner would hold an independent statutory position within the Australian Human Rights Commission. At the time of writing, these changes have not taken place. In this Report, the ALRC uses the terms 'Privacy Commissioner' and 'Commissioner' to refer to the person exercising the privacy functions under the *Privacy Act*.

2 ACCAN, *Submission 106*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

3 Australian Privacy Foundation, *Submission 110*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

4 Australian Privacy Foundation, *Submission 110*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

5 Office of the Australian Information Commissioner, *Submission 90*.

complaints about breaches of information privacy. The *Privacy Act* currently provides for complaints to be made to the Commissioner where there may have been an 'interference with the privacy of an individual'.[6] Under the Act, an interference with the privacy of an individual will have occurred where there has been a breach of:

- any of the Australian Privacy Principles (APPs);[7]
- a registered APP code;[8]
- the credit reporting provisions or the registered CR code;[9]
- certain rules relating to tax file numbers;[10] or
- certain provisions of other legislation, where that legislation provides that a particular act or conduct is an interference with the privacy of an individual for the purposes of the *Privacy Act*.[11]

16.7 The *Privacy Act* could be amended to provide that a serious invasion of privacy would also be an interference with the privacy of an individual. This approach was suggested by Professor Graham Greenleaf, who submitted that, if an Act providing for the tort for serious invasions of privacy were enacted:

> a new sub-section 13(6) should be added to the *Privacy Act 1988*: '(6) A serious invasion of privacy under the [Act providing the statutory tort] is an interference with the privacy of an individual …'[12]

16.8 In the event that an interference with the privacy of an individual occurs, the Commissioner has the power to receive and investigate a complaint from the individual whose privacy has been interfered with, or to begin an 'own motion investigation' of the interference.[13] Following an investigation, the Commissioner may make a determination including various declarations, such as a declaration that the respondent to the complaint must take specified actions, a declaration that the respondent must take steps to redress any loss or damage suffered by the complainant, or a declaration that the complainant is entitled to a specified amount of compensation.[14] A determination following an investigation is enforceable through the Federal Court and Federal Circuit Court, on application of either the complainant or the Commissioner.[15] If a serious invasion of privacy was also an interference with the privacy of an

---

6 *Privacy Act 1988* (Cth) s 36.
7 Ibid s 13(1).
8 Ibid.
9 Ibid s 13(2).
10 Ibid s 13(4).
11 An interference with the privacy of an individual can arise, for example, under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 35L.
12 G Greenleaf, *Submission 76*. As noted in Professor Greenleaf's submission, if a new section in the *Privacy Act* referred to 'an act', a range of exemptions, such as the media exemption under s 7B(4), would take effect, limiting the effect of the new provisions.
13 *Privacy Act 1988* (Cth) ss 36, 40.
14 Ibid s 52(1). Similar declarations may be made in the case of an own motion investigation: ibid s 52(1A).
15 *Privacy Act 1988* (Cth) s 55A.

individual under the *Privacy Act*, these same determinations could be made following a complaint to the Commissioner about a serious invasion of privacy.

16.9 Further consequences of an interference with the privacy of an individual under the *Privacy Act* include:

- where an interference with the privacy of an individual is 'serious' or 'repeated', the Commissioner is empowered to seek civil pecuniary penalties from the Federal Court or Federal Circuit Court;[16] and
- where a person has engaged in, or is engaging in, conduct that contravenes the Act, an individual or the Commissioner may apply to the Federal Court or the Federal Circuit Court for an injunction.[17]

16.10 The media, small businesses and individuals are not exempt from liability under the tort for serious invasions of privacy discussed in Part 2 of this Report. However, they are generally exempt from regulation under the *Privacy Act*.[18] If the Commissioner's functions were extended to hear complaints about serious invasions of privacy, this should include complaints about invasions of privacy by the media, small business and individuals. There would be little value in extending the Commissioner's powers if the existing exemptions also applied to complaints made under the extended powers. The amendments to the *Privacy Act* would need to make this clear.

16.11 Before any extended powers were conferred on the Commissioner, consideration would need to be given to whether or not the extended powers would require the Commissioner to exercise a judicial power. The *Australian Constitution* restricts the conferral of judicial powers on non-judicial bodies.[19] Although 'judicial power' has not been exhaustively defined, one characteristic of a judicial power is its binding nature.[20] A determination under the *Privacy Act* complaints process is not binding, since it must be enforced through action in the Federal Court or Federal Magistrates Court. This suggests that the *Privacy Act* does not confer judicial powers on the Commissioner.[21]

Deletion, removal and de-identification

16.12 The Commissioner's existing powers in relation to an interference with the privacy of an individual include a power to make a declaration that the respondent

16 Ibid ss 13G, 80W.

17 Ibid s 98. This provision appears to be rarely used. However, it provides a useful means for an individual to seek relief for a breach of the *Privacy Act*.

18 For the media exemption, see *Privacy Act* s 7B(4). For the small business exemption, see *Privacy Act* ss 6C(1), 6D. For the exemption for individuals, see *Privacy Act* s 16. Individuals will also generally fall outside the definition of relevant types of entities; see, for example, *Privacy Act* s 6(1) (definition of 'APP entity').

19 *R v Kirby; ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254.

20 *Brandy v Human Rights & Equal Opportunity Commission* (1995) 183 CLR 245, 268 (Deane, Dawson, Gummow, McHugh JJ).

21 An example of a regulator being found to have exercised a judicial function can be found in *Today FM (Sydney) v Australian Communications and Media Authority* (2014) 307 ALR 1. There, the Full Federal Court found that the Australian Communications and Media Authority had exercised a judicial power in finding that a broadcaster had breached a licence condition by committing a criminal offence.

'must not repeat or continue such conduct'[22] or a declaration that the respondent 'must take specified steps within a specified period to ensure that such conduct is not repeated or continued'.[23] It appears that such declarations may require the respondent to delete, remove or de-identify personal information.

16.13 A number of stakeholders supported the introduction of a regulator take-down mechanism.[24] However, there is a risk that such a system may have an undesirably chilling effect on online freedom of expression, and any such power would need to balance the interests of the complainant against the interests of the party in publishing the material and broader public interests. The power would need to be exercised with caution.

16.14 The existing availability of declarations that a respondent to a complaint not repeat or continue the conduct complained about may provide a suitable mechanism for individuals to seek to have information removed, while avoiding the chilling effect that may come from other take-down mechanisms. There may be no need to confer substantial new powers on the Commissioner, beyond the power to investigate complaints about serious invasions of privacy. Furthermore, a declaration that a respondent must not repeat or continue the conduct complained about would not, by itself, be enforceable; the complainant would need to apply to the Federal Court or Federal Circuit Court for enforcement if the respondent refused to comply with the Commissioner's declaration.

16.15 Several stakeholders were opposed to any take-down mechanism on the grounds that such a mechanism may, in some cases, be ineffective.[25] The Australian Mobile Telecommunications Association and Communications Alliance submitted that, given the speed and volume at which content is created and published online,

> the implementation of such a system is likely to be impossible to comply with and costly and time-consuming for government and business, as well as being ineffective in relation to user-generated content.[26]

16.16 Several other organisations noted the difficulty of effectively removing information that has become more widely available,[27] or where the respondent is located overseas.[28]

---

22 *Privacy Act 1988* (Cth) s 52(1)(b)(i).

23 Ibid s 52(1)(b)(ia).

24 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Pirate Party of Australia, *Submission 119*; Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Redfern Legal Centre, *Submission 94*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*.

25 Telstra, *Submission 107*; AMTACA, *Submission 101*; Australian Bankers' Association, *Submission 84*.

26 AMTACA, *Submission 101*.

27 Australian Communications and Media Authority, *Submission 121*; Pirate Party of Australia, *Submission 119*.

28 Australian Communications and Media Authority, *Submission 121*; Pirate Party of Australia, *Submission 119*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Office of the Australian Information Commissioner, *Submission 90*.

16.17 The ALRC acknowledges that a take-down mechanism may have limited effect in cases where material has been widely disseminated or where material is hosted overseas. However, the ALRC considers that the possibility of the mechanism having limited effect in some cases is not, in itself, a reason not to make the mechanism available in those cases where it may be effective. This is particularly the case given that the Commissioner is already empowered to make the relevant declarations under the existing provisions of the *Privacy Act*.

Complaints about media invasions of privacy

16.18 In the Discussion Paper, the ALRC proposed an extension of the powers of the Australian Communications and Media Authority (ACMA). However, the ALRC has concluded that such declarations would be more appropriately made by the Privacy Commissioner.

16.19 The proposed extension would have allowed the ACMA to make a declaration that the complainant was entitled to a specified amount of compensation, in response to a complaint about a serious invasion of privacy in breach of a broadcasting code of conduct. This would have been equivalent to the powers of the Privacy Commissioner.

16.20 Although the Commissioner already has such powers under the *Privacy Act*,[29] the relevant provisions of the *Privacy Act* do not apply to a media organisation acting in a journalistic capacity if the organisation has publicly committed to observing privacy standards.[30] The result is that an individual whose privacy is invaded by a broadcaster has little access, if any, to regulatory mechanisms providing for compensatory redress.

16.21 The ACMA's powers with respect to broadcasting codes of conduct are provided under the *Broadcasting Services Act 1992* (Cth). These powers are primarily exercised by promoting self-regulation—in which industry members regulate themselves under industry guidelines, codes or standards; and co-regulation—in which industry members develop guidelines, codes or standards that are enforceable under legislation.

16.22 If a code is breached, the ACMA may: determine an industry standard;[31] make compliance with the code a condition of the broadcaster's licence;[32] or accept an enforceable undertaking from the broadcaster that the broadcaster will comply with the code.[33] Further consequences exist, including civil penalties, criminal penalties and suspension or cancellation of a broadcaster's licence, for a breach of a standard,[34] a licence condition[35] or an enforceable undertaking.[36] If a complaint is made against the

---

29 Under *Privacy Act* s 52(1A)(d), the Australian Information Commissioner, in response to a complaint, may make a determination including a declaration that the respondent pay an amount of compensation to the complainant.

30 *Privacy Act 1988* (Cth) s 7B(4).

31 *Broadcasting Services Act 1992* (Cth) s 125.

32 Ibid s 44.

33 Ibid s 205W.

34 Ibid pt 9B div 5.

35 Ibid pt 10 div 3.

36 Ibid pt 14D.

ABC or SBS, the ACMA may recommend that the broadcaster take action to comply with the relevant code, or that the broadcaster take other action including publishing an apology or retraction.[37]

16.23 There was significant opposition from broadcasters and media organisations to the proposal to extend the ACMA's powers. A key argument among broadcasters was that the proposal was inconsistent with the ACMA's existing role as the manager of a co-regulatory scheme which has the goal of 'encouraging broadcasters to reflect community standards'.[38] The Australian Subscription Television and Radio Association (ASTRA) submitted, for example, that

> Such a proposal would represent a significant shift in the functions and powers of the ACMA. The ACMA does not currently have the power to order compensation be paid to an individual in relation to a breach of any broadcasting code of practice, broadcasting licence condition or any other obligation on broadcasters established under the *Broadcasting Services Act 1992* (BSA). This does not represent a 'limitation' of the ACMA's powers under the BSA—rather, it reflects … the intention of the regulatory framework for broadcasting established by Parliament.[39]

16.24 Stakeholders—including the ACMA itself—were also concerned that, if the ACMA were empowered to suggest compensation for invasions of privacy, there would be increased fragmentation of privacy protections. This fragmentation would result in confusion and complexity for individuals and organisations:

- different regulators would regulate privacy in different sectors;[40]
- the new power would apply only to breaches of broadcasting codes involving serious invasions of privacy, and not to other breaches of the codes;[41]
- within the media sector, different regulatory schemes would apply to different forms of media.[42]

16.25 The risks of fragmentation under the proposed ACMA power are, to a large extent, an unavoidable consequence of the fragmented nature of media regulation in Australia. While the ACMA has powers relating to broadcast media under the *Broadcasting Services Act*, regulation of non-broadcast media is a matter of self-regulation by the Australian Press Council.

16.26 Although a number of stakeholders were supportive of the proposed ACMA power,[43] the ALRC has determined, in view of the changes to the existing regulatory landscape that would be involved, not to proceed with the proposal.

---

37 Ibid ss 150–152.
38 Australian Communications and Media Authority, *Submission 121*.
39 ASTRA, *Submission 99*. See also SBS, *Submission 123*; Free TV, *Submission 109*.
40 Office of the Australian Information Commissioner, *Submission 90*.
41 Australian Communications and Media Authority, *Submission 121*.
42 SBS, *Submission 123*.
43 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; G Greenleaf, *Submission 76*; D Butler, *Submission 74*.

16.27 The ACMA suggested, as an alternative to the proposed new power, that the ACMA should be empowered:

> [to] refer found privacy breaches to the [Office of the Australian Information Commissioner] to make a determination as to the seriousness of the breach, to provide for conciliation and to make [a] declaration as to the amount of any compensation payable.[44]

16.28 Noting that the ACMA's role, as discussed above, is not to provide individual redress, the ALRC agrees that the Privacy Commissioner is an appropriate body to make declarations relating to compensation for serious invasions of privacy. However, if the Commissioner's powers are extended to include investigating complaints about serious invasions of privacy by broadcasters or other media, the media exemption of the *Privacy Act* should not apply in respect of complaints about serious invasions of privacy. The media exemption could, however, continue to apply in respect of information privacy under others parts of the *Privacy Act*.

Conciliation process

16.29 An alternative to extending the Commissioner's existing investigation powers is a conciliation process operated by the Commissioner. Such a conciliation process could be similar to that used by the Australian Human Rights Commission (AHRC). Under pt IIB of the *Australian Human Rights Commission Act 1986* (Cth), the President of the AHRC may attempt to conciliate a complaint alleging unlawful discrimination. In certain circumstances—for example, where the President of the AHRC is satisfied that there is no reasonable prospect of the matter being settled by conciliation—a complaint may be taken to the Federal Court or the Federal Circuit Court.[45]

16.30 The Law Institute of Victoria expressed a preference for this type of model, whereby

> the Privacy Commissioner would be providing alternative dispute resolution services, rather than making a finding about the claim. If the dispute is not resolved, the plaintiff would be required to pursue the claim through the courts.[46]

16.31 A conciliation process would not be binding on parties. However, conciliation may lead to satisfactory outcomes for both parties, without the need to resort to court proceedings. In the event that conciliation was unsuccessful, the complaint could be taken to a court under the tort for serious invasions of privacy, if that statutory tort were enacted.

16.32 The conciliation process would thus provide an initial low cost mechanism for resolving disputes. Such a process need not be mandatory. However, the ALRC recommends that a failure to make a reasonable attempt at conciliation should be a factor considered by a court in the event that damages were to be awarded.[47]

---

44 Australian Communications and Media Authority, *Submission 121*.

45 The usefulness of the AHRC's conciliation function as a model was noted by the Media and Communications Committee of the Law Council of Australia, *Submission 124*.

46 Law Institute of Victoria, *Submission 96*.

47 See Ch 12 and in particular Rec 12–2.

Amicus curiae and intervener functions

Recommendation 16–2 The following functions should be conferred on the Privacy Commissioner:

(a) to assist a court as amicus curiae, where the Commissioner considers it appropriate, and with the leave of the court; and

(b) to intervene in court proceedings, where the Commissioner considers it appropriate, and with the leave of the court.

16.33 The ALRC recommends that the Privacy Commissioner be given new functions to act as amicus curiae ('friend of the court') or to intervene in legal proceedings relating to serious invasions of privacy. These functions would be additional to a range of existing functions conferred on the Commissioner under *Privacy Act 1988* (Cth) ss 27–29, including: preparing guidance about the Act; monitoring the privacy impacts of new laws; and providing advice about the operation of the Act.

16.34 These amicus curiae and intervener functions would be similar to functions conferred on other administrative bodies—such as the Australian Competition and Consumer Commission (ACCC), the Australian Securities and Investments Commission (ASIC) and the AHRC.

16.35 Stakeholders who commented on the ALRC's proposal were generally supportive of the Commissioner being given amicus curiae and intervener functions.[48] The Office of the Australian Information Commissioner (OAIC) suggested that it should be given amicus curiae and intervener roles in its submission to the Issues Paper.[49] In its submission to the Discussion Paper, the OAIC noted that amicus curiae and intervener roles would be particularly appropriate if the OAIC had a greater role in hearing complaints about serious invasions of privacy.[50]

16.36 It is likely that, if a statutory cause of action for serious invasions of privacy were enacted, there would be an increase in the number of claims relating to the intentional disclosure of personal information. In such cases, the Commissioner may be in a position to assist the court as amicus curiae, or to represent the Commissioner's interests as an intervener.

---

48 T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; G Greenleaf, *Submission 76*.

49 Office of the Australian Information Commissioner, *Submission 66*.

50 Office of the Australian Information Commissioner, *Submission 90*.

An amicus curiae function for the Commissioner

16.37 The role of an amicus curiae is to assist the court 'by drawing attention to some aspect of the case which might otherwise be overlooked.'[51] An amicus curiae may 'offer the Court a submission on law or relevant fact which will assist the Court in a way in which the Court would not otherwise have been assisted'.[52] The amicus is not a party to the proceedings and is not bound by the outcome of the proceedings. This role does not extend to introducing evidence to the court, although an amicus may be permitted to lead non-controversial evidence in order to 'complete the evidentiary mosaic'.[53]

16.38 An example of legislation conferring an amicus curiae function on an administrative body is s 46PV of the *Australian Human Rights Commission Act 1986* (Cth). This section allows an individual ('special-purpose') Commissioner within the AHRC to act as amicus curiae, with the court's leave:

> (1) A special-purpose Commissioner has the function of assisting the Federal Court and the Federal Circuit Court, as amicus curiae, in the following proceedings under this Division:
>
> (a) proceedings in which the special-purpose Commissioner thinks that the orders sought, or likely to be sought, may affect to a significant extent the human rights of persons who are not parties to the proceedings;
>
> (b) proceedings that, in the opinion of the special-purpose Commissioner, have significant implications for the administration of the relevant Act or Acts;
>
> (c) proceedings that involve special circumstances that satisfy the special-purpose Commissioner that it would be in the public interest for the special-purpose Commissioner to assist the court concerned as amicus curiae.

16.39 Importantly, an amicus curiae does not have a legal interest in the outcome of the proceedings. Any person with a legal interest in proceedings may, with the leave of the court, intervene in the proceedings.

An intervener function for the Commissioner

16.40 The role of amicus curiae can be distinguished from the role of an intervener. While the role of amicus is to assist the court, the role of an intervener is to represent the intervener's own legal interests in proceedings.

16.41 An intervener's legal interests may be affected in a number of ways. The intervener's interests may be directly affected by the court's decision. For example, a decision about the property interests of the parties to proceedings might also affect the property interests of the intervener. The intervener's interests may also be indirectly affected: for example, the court's decision might have an effect on the future

---

51 *Bropho v Tickner* (1993) 40 FCR 165, 172 (Wilcox J). On the role of an amicus curiae generally, see Australian Law Reform Commission, *Beyond the Door-Keeper: Standing to Sue for Public Remedies*, Report 78 (1996) Ch 6.

52 *Levy v Victoria* (1997) 189 CLR 579, 604 (Brennan CJ).

53 *Bropho v Tickner* (1993) 40 FCR 165, 172 (Wilcox J).

interpretation of laws affecting the intervener.[54] Under the ALRC's recommendation, a court might, for example, give leave to the Commissioner to intervene in a case that would have future repercussions for the work of the Commissioner.

16.42 Functions to intervene are conferred upon a number of administrative bodies. For example, s 11(1)(o) of the *Australian Human Rights Commission Act* confers an intervention function on the AHRC:

> where the Commission considers it appropriate to do so, with the leave of the court hearing the proceedings and subject to any conditions imposed by the court, to intervene in proceedings that involve human rights issues.[55]

16.43 The ACCC has an intervention function in relation to proceedings under the *Competition and Consumer Act 2010* (Cth).[56] ASIC has an intervention function in relation to proceedings about consumer protection in financial services.[57]

Deletion of personal information

16.44 Several submissions to the Issues Paper noted that the harm caused by a serious invasion of privacy in the digital era will often increase the longer private information remains accessible.[58] It is therefore important that individuals be able to exercise a degree of control over their personal information, especially information that they may themselves have provided previously. In particular, individuals should be empowered to have their personal information destroyed—or, at a minimum, de-identified—when appropriate.

16.45 In the Discussion Paper, the ALRC proposed that a new APP be inserted into the *Privacy Act*, that would:

- require APP entities to provide a simple mechanism for an individual to request destruction or de-identification of personal information that the individual had provided to the entity; and
- require APP entities to take reasonable steps in a reasonable time to comply with such a request, subject to suitable exceptions, or to provide the individual with reasons for non-compliance.

16.46 The ALRC argued that the proposed APP would complement existing APPs that require APP entities to correct personal information (the correction principle)[59] and to destroy or de-identify personal information when it is no longer required for a relevant

---

54 *Levy v Victoria* (1997) 189 CLR 579, 601–602 (Brennan CJ).

55 The Australian Human Rights Commission also has intervention functions, see for example, *Australian Human Rights Commission Act 1986* (Cth) s 31(j); *Sex Discrimination Act 1984* (Cth) s 48(1)(gb); *Racial Discrimination Act 1975* (Cth) s 20(e); *Disability Discrimination Act 1992* (Cth) s 67(1)(1); *Age Discrimination Act 2004* (Cth) s 53(1)(g).

56 *Competition and Consumer Act 2010* (Cth) s 87CA.

57 *Australian Securities and Investments Commission Act 2001* (Cth) s 12GO.

58 National Children and Youth Law Centre, *Submission 61*; Google, *Submission 54*; Australian Privacy Foundation, *Submission 39*; B Arnold, *Submission 28*.

59 *Privacy Act 1988* (Cth) APP 13.

purpose (the security principle).[60] Although the existing APPs provide some protection, they do not incorporate a mechanism allowing individuals to request destruction or de-identification.

16.47 The proposal was supported by a number of stakeholders.[61] Others were opposed to it,[62] noting the existing correction and security principles[63] and the need to retain personal information for business purposes, such as billing.[64] Some stakeholders were not opposed to the proposal, subject to particular concerns being met.[65]

16.48 The OAIC opposed the proposal. The OAIC noted that it would not be relevant to most information held by Australian Government agencies due to the retention requirements of the *Archives Act 1983* (Cth). The OAIC also noted that, in addition to the existing correction and security principles, other principles restrict the circumstances in which an APP entity may collect or disclose information:[66]

> The requirement in the proposed APP for an organisation to destroy or de-identify the personal information, in circumstances where the organisation is still authorised to use or disclose it under the Privacy Act … has the potential to impose a significant burden on the organisation and disrupt its business practices. The OAIC considers that the existing measures in the APPs balance the need to give an individual control over the handling of their personal information with the regulatory burden on entities when carrying out their functions and activities, and that the additional burden in the proposed new APP is unjustified and unnecessary.[67]

16.49 The OAIC also submitted that, rather than introducing a new APP into the *Privacy Act*, the OAIC could

> issue additional guidance on an entity's obligations under the existing APPs to destroy or de-identify personal information and good privacy practice when an individual requests the entity to destroy or de-identify their personal information.

16.50 The ALRC accepts that the existing APPs require the destruction or de-identification of personal information in many circumstances. However, there are scenarios in which an APP entity may be able to retain personal information even after the individual has ceased their business relationship with the APP entity. For example, if the purpose of the collection includes the APP entity's own statistical research, it is not clear that the entity would be required to destroy or de-identify the information

---

60 Ibid APP 11.2.

61 T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Communications Consumer Action Network, *Submission 106*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; G Greenleaf, *Submission 76*.

62 Telstra, *Submission 107*; AMTACA, *Submission 101*; ASTRA, *Submission 99*; Office of the Australian Information Commissioner, *Submission 90*; Interactive Games and Entertainment Association, *Submission 86*; Australian Bankers' Association, *Submission 84*.

63 AMTACA, *Submission 101*; Interactive Games and Entertainment Association, *Submission 86*.

64 ASTRA, *Submission 99*.

65 Australian Interactive Media Industry Association (AIMIA), *Submission 125*; Insurance Council of Australia, *Submission 102*.

66 *Privacy Act 1988* (Cth) APPs 3, 6.

67 Office of the Australian Information Commissioner, *Submission 90*.

unless and until the research was concluded, regardless of the duration or purpose of the research.

16.51 However, the ALRC accepts that the introduction of a new APP may require further consideration of the existing APPs, and that the effect of the recent reforms of the *Privacy Act* should be determined before further reforms take place.[68] The ALRC is not, therefore, recommending the introduction of a new APP. The ALRC remains concerned, however, that the existing APPs do not require an entity to provide a simple mechanism allowing an individual to request the destruction or de-identification of personal information.

Review of the small business exemption

16.52 The APPs under the *Privacy Act* regulate the handling of personal information by APP entities: government agencies and organisations.[69] Notably, small businesses with an annual turnover of less than $3 million[70] are exempt from the definition of 'organisation' and hence from the ambit of the APPs unless, for instance:

- the small business trades in personal information;
- the small business handles health information; or
- the small business operator notifies the OAIC in writing of its desire to be treated as an organisation.[71]

16.53 In its 2008 report, *For Your Information*, the ALRC recommended that the small business exemption be removed from the *Privacy Act*. Several stakeholders, in submissions to the ALRC's current Inquiry, noted that the exemption remains in the *Privacy Act*, and that the removal of the exemption would have substantial benefits for the protection of privacy.[72]

16.54 Ensuring that small businesses handle personal information in an appropriate way may be particularly important in the digital era. A small business in the digital era can readily collect personal information through, for example, software on mobile phones or websites.[73]

16.55 The ALRC considers that the small business exemption should be given further consideration, particularly given the growth of digital communications and the digital economy since 2008. The ALRC acknowledges that simply removing the small

---

68 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
69 *Privacy Act 1988* (Cth) s 6(1) (definition of 'APP entity').
70 Ibid ss 6C, 6D.
71 Ibid ss 6D, 6E, 6EA.
72 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 39–1.
73 'Mobile Apps' (Occasional paper 1, Australian Communications and Media Authority, May 2013); 'The Cloud—services, Computing and Digital Data' (Occasional paper 3, Australian Communications and Media Authority, June 2013); 'Mobile Privacy: A Better Practice Guide for Mobile App Developers' (Office of the Australian Information Commissioner, September 2013).

business exemption would increase compliance costs for small businesses. However, options other than simply removing the exemption are available.

16.56 The Productivity Commission may be well-placed to investigate the likely impacts on small businesses if the small business exemption were removed, or if other options for protecting personal information held by small businesses were introduced. Such an investigation could give detailed consideration to the application of data protection laws to small businesses in other jurisdictions[74] as well as other options for improving the protection of personal information held by small business. These options might include, for example, the introduction of an accreditation scheme to encourage small businesses to opt in[75] to the *Privacy Act* in order to demonstrate a commitment to good privacy practices, or a limitation of the small business exemption so that small businesses handling sensitive information[76] or financial information would not be exempt from the Act.

74 For example, small business are bound by the *Data Protection Act 1998* (UK).

75 Small businesses may elect to be treated as organisations under s 6EA of the *Privacy Act 1988* (Cth).

76 Sensitive information includes personal information about an individual's racial or ethnic origin, political opinions, membership of political associations, religious beliefs or affiliations, philosophical beliefs, professional or union membership, sexual orientation or practices or criminal record, as well as health information, genetic information, and certain types of biometric information: Ibid s 6(1) (definition of 'sensitive information').