Australian Government
Office of the Australian Information Commissioner

Serious invasions of privacy in the digital era

Submission to the Australian Law Reform Commission on Discussion Paper 80

May 2014

Prof John McMillan, Australian Information Commissioner
Timothy Pilgrim, Privacy Commissioner

Contents

Introduction

The Office of the Australian Information Commissioner (the OAIC) welcomes the Australian Law Reform Commission's release of 'Serious invasions of privacy in the digital era – Discussion Paper 80' (DP 80).[1]

The Office of the Australian Information Commissioner

The OAIC was established by the *Australian Information Commissioner Act 2010* (Cth) (the AIC Act) and commenced operation on 1 November 2010.

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The OAIC brings together the functions of government information policy and independent oversight of privacy protection and freedom of information (FOI).

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth), and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Cth) (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Structure of this submission

The OAIC's comments on DP 80 are structured as follows:

- a 'General comments in response to DP 80' section which discusses the OAIC's general observations in response to DP 80, including on the proposed tort for serious invasion of privacy
- a 'Comments in response to DP 80 proposals and questions' section which outlines the OAIC's comments in response to the particular proposals and questions raised in DP 80. The OAIC has only commented on proposals or questions that relate to issues on which the OAIC has not previously commented during this inquiry and is able to offer expertise.

[1] Australian Law Reform Commission, *Serious invasions of privacy in the digital era – Discussion Paper 80*, available at <www.alrc.gov.au/publications/serious-invasions-privacy-dp-80>.

General comments in response to DP 80

The OAIC supports the extension of privacy law to cover serious invasion of privacy. This extension would be consistent with Australia's international obligations in relation to privacy protection.[2]

In the context of developing a serious privacy invasion redress mechanism, the OAIC particularly supports:

- the ALRC's guiding principle 8 that 'justice to protect privacy should be accessible'.[3] Accessibility is important to ensuring that the new privacy invasion redress mechanism delivers the intended benefits and meets community expectations regarding increased privacy protections
- the adoption of laws that are uniform in application and jurisdiction,[4] and are technology neutral.[5] Uniform laws will contribute to consistent privacy regulation and avoid further fragmentation in privacy protections.[6] Technologically neutral mechanisms will ensure the mechanisms are adaptable and are able to address privacy invasive acts and practices that may emerge in the future as a result of technological developments and consequential social trends.

DP 80 sets out a proposed legal design for a tort of serious privacy invasion actionable straight to the courts (a 'court model'). However, for the reasons outlined in the OAIC's submission in response to the ALRC's Issues Paper 43,[7] the OAIC maintains its position that addressing serious privacy invasion would be most effectively achieved by amending the existing privacy regulatory framework in the *Privacy Act 1988* (Cth) to extend the complaint framework in that Act to cover serious invasions of privacy (termed the 'complaints model for serious privacy invasion').[8]

The complaints model for serious privacy invasion would provide benefits over a court model in relation to access to justice, by providing a method for fast, informal and low-

---

2 For example, see Article 17 of the *International Covenant on Civil and Political Rights*. For more information on how this extension is consistent with Australia's international obligations, see OAIC December 2013, *Serious invasions of privacy in the digital era – submission to the Australian Law Reform Commission* (OAIC submission on Issues Paper 43), available at: <www.oaic.gov.au/news-and-events/submissions/privacy-submissions/serious-invasions-of-privacy-in-the-digital-era>.

3 See DP 80 at paragraphs [2.33]-[2.35].

4 See guiding principle 7: 'privacy laws should be coherent and consistent', DP 80 at paragraph [2.26].

5 See guiding principle 5: 'privacy laws should be adaptable to technological change', DP 80 at paragraph [2.21]-[2.22].

6 Existing fragmentation in privacy protections in Australia arises for a number of reasons, including that:
- the *Privacy Act 1988* (Cth) only regulates information privacy, and protections for other types of privacy generally only cover specific acts and practices
- information privacy protections differ between Commonwealth and state/territory jurisdictions
- various entities and acts and practices are exempt from the *Privacy Act 1988* (Cth).

7 OAIC submission on Issues Paper 43: <www.oaic.gov.au/news-and-events/submissions/privacy-submissions/serious-invasions-of-privacy-in-the-digital-era>.

8 While complaints under the complaints model for serious privacy invasion would initially be made to the OAIC, the model still envisages a role for the courts, such as the OAIC referring a question of law to the court for guidance, or the OAIC terminating an investigation if satisfied the matter involves an issue of public importance that should be considered by the court.

cost resolution of disputes, generally through conciliation. In addition, complainants would have access to the OAIC's existing privacy expertise and processes, and expertise in privacy complaint conciliation. Both the Privacy Act and the OAIC and Privacy Commissioner have high visibility in the Australian community and are regularly approached by the community about privacy concerns. Extending the existing framework of the Privacy Act to apply a complaints model to serious invasions of privacy would therefore be a logical step that builds on a successful and accessible model for dispute resolution.

Additionally, the OAIC notes the recent Productivity Commission draft report on 'Access to Justice Arrangements'[9] which identifies the many benefits of the ombudsmen[10] model in the context of access to justice,[11] and concludes that ombudsman 'have filled an important gap in the civil justice landscape – a mechanism for resolving low value disputes'.

By not adopting the complaints model for serious privacy invasion and instead proposing a court model, the OAIC is concerned that the ALRC's tort proposal will not be accessible for the vast majority of individuals.

In addition, not adopting the complaints model for serious privacy invasion, together with the design of the ALRC's tort, means the proposals put forward by the ALRC may lead to further fragmentation in privacy protections, as outlined further in this submission. For example:

- while the proposal to allow courts at all levels to hear serious privacy invasion matters[12] is designed to increase access to justice, this approach risks the emergence of differing judicial interpretations of the legislation in each jurisdiction. This would further fragment privacy protections across Australia.[13] Instead, the complaints model for serious privacy invasions would deliver greater access to justice than granting jurisdiction to lower courts, while at the same time promoting consistent development and application of the law by generally confining the interpretation of the law to the OAIC and the federal courts
- while take-down powers may be an effective tool in cases of serious privacy invasion, those powers may ultimately be conferred on a regulator with no other significant role in dealing with serious privacy invasions. If both the ALRC's court

9 Productivity Commission 2014, *Access to Justice Arrangements (draft report)*, Productivity Commission website: <www.pc.gov.au/projects/inquiry/access-justice/draft>.

10 The Australian Information Commissioner is identified as an 'ombudsman' for the purposes of the draft report (see Appendix D).

11 These benefits include:
- providing a mechanism for resolving low value disputes
- helping to overcome power imbalances
- providing a simple to use system and removing the need for professional representatives
- an approach that actively pursues the resolution of disputes rather than leaving primary control to the parties as has occurred historically in courts
- providing a mechanism for identifying and addressing systemic issues.

12 See Proposal 9-1, DP 80.

13 See footnote 4 for further detail.

model and the take-down mechanism are introduced, this may lead to further fragmentation in privacy regulation

- a court model which is inaccessible to many individuals will create inconsistency in the remedies which individuals are realistically able to achieve. An individual with limited resources may be unable to obtain the appropriate remedy for a serious invasion of their privacy, while a well-resourced individual may obtain that remedy for a similar privacy invasion. This inconsistency would be minimised by the complaints model for serious privacy invasion given it provides informal and low-cost resolution of disputes, with a focus on early dispute resolution
- conferring on the Australian Communications and Media Authority (ACMA) the power to award compensation for serious privacy invasions by broadcasters (where the conduct also breaches a relevant broadcasting code) increases fragmentation in privacy protections by introducing a complaints model that is only available for a narrow subset of serious privacy invasions (see the OAIC's response below to Proposal 15-1)
- confining the privacy invasion action to intrusion upon seclusion and misuse of private information increases fragmentation in privacy protections by not addressing all serious privacy invasions and could limit the adaptability of the mechanism (see the OAIC's response below to Proposal 5-1).

While the OAIC's preference is for the complaints model for serious privacy invasion, the OAIC's comments below relate to selected proposals and questions that have been put forward by the ALRC in DP 80.

Comments in response to DP 80 proposals and questions

Proposal 5-1: The new tort should be confined to invasions of privacy by:

- **intrusion upon the plaintiff's seclusion or private affairs (including by unlawful surveillance); or**
- **misuse or disclosure of private information about the plaintiff (whether true or not).**

The OAIC supports the enactment of a single and comprehensive tort rather than confining the tort to intrusion upon seclusion and misuse or disclosure of private information.

The OAIC has two main concerns about confining the tort in the proposed manner:

- enacting a limited tort that deals with only specific types of privacy invasion risks leaving gaps in privacy protection. For example, it is not clear that this proposed tort would provide a remedy in the case of serious invasion of an individual's bodily privacy (such as in the case of unauthorised bodily testing). While the majority of serious privacy invasions may fall within the two proposed categories, some will not and this will create further fragmentation in privacy protections

- a limited tort may be less able to adapt and apply flexibly to changing technologies and practices than a more general and comprehensive tort that applies to all serious invasions of privacy.

Question 10-2: Should the new Act provide for a defence of necessity?

The OAIC considers that, in many instances, a defence of necessity would not be required because elements of the proposed tort would already protect a respondent. For example, where a respondent feels compelled to invade an individual's privacy in order to prevent or reduce the occurrence of a more serious harm, it is likely that at least one of the following would apply so that an actionable invasion of privacy has not occurred:

- the plaintiff would not have a reasonable expectation of privacy
- the invasion would not be considered to meet the requisite level of 'seriousness'
- when public interests are balanced, another public interest would outweigh the individual's right to privacy in that situation.

The OAIC acknowledges that there may be some instances where the elements of a proposed tort would not protect a respondent, such as where the serious invasion of privacy is carried out in the interests of a particular individual or a smaller group. However, the OAIC is concerned that a defence of 'necessity' would provide a wide-ranging defence. Further, 'necessity' is a vaguely described defence that does not give guidance on why a serious invasion of privacy might be acceptable in a particular circumstance.

Instead, the OAIC suggests that consideration could be given to providing a more targeted defence. For example, a defence could be provided that is similar to exceptions in the Privacy Act that allow for the collection, use or disclosure of personal information where the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health and safety.[14]

Question 10-3: What conditions should internet intermediaries be required to meet in order to rely on this safe harbour scheme?

Generally, the OAIC considers that internet intermediaries should take reasonable steps to prevent serious privacy invasions from occurring via their services.[15] Further, in the event that a serious invasion of privacy does occur via an intermediary's service, the OAIC considers that the intermediary should take reasonable steps to assist the affected individual and law enforcement with resolving the matter and mitigating its impact on the individual.

[14] See s 16A item 1 of the *Privacy Act 1988*.

[15] Proposal 10-7 in DP 80 is that the new Act should provide a safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their service.

Other stakeholders may be better placed to specify particular conditions for any such scheme, but at a minimum the OAIC would expect that internet intermediaries would be required to:

- comply with applicable privacy obligations, including the Privacy Act and industry codes
- reasonably cooperate with and assist the relevant regulator with locating and pursuing the wrongdoer
- have appropriate terms of service, which take account of the potential for users to invade privacy
- take reasonable steps to monitor and enforce compliance with those terms of service. For example, if a particular offence is being increasingly committed via a particular intermediary's service, it would be reasonable for the intermediary to monitor this. Further, where a particular action breaches the intermediary's terms of service, the intermediary should take appropriate actions in response, such as terminating the users right to the service
- integrate reasonable privacy protections into their systems and processes
- be able to evidence that they have taken reasonable steps to:
    - encourage users to protect and respect the privacy of others
    - implement systems to deal with privacy enquiries and complaints from individuals in a timely and reasonable manner
- comply with any take-down or other regulatory orders in relation to privacy invasions in the prescribed timeframes and manner, and
- be able to otherwise evidence that they have taken reasonable steps to prevent the occurrence of serious invasions of privacy.

Acknowledging the different purposes, the OAIC notes that the US-EU Safe Harbor scheme (which allows companies in the European Union (EU) to send personal data to United States (US) companies provided that the US company adheres to the 7 principles outlined in the EU directive) has received significant criticism from the European Commission, for example:[16]

- specific EU Member States' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation (industry has raised similar concerns, referring to distortions of competition due to a lack of enforcement)
- the framework lacks transparency and active enforcement, resulting in some Safe Harbor self-certified companies not complying with the Safe Harbor Principles in practice

[16] See <ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf>; <www.hldataprotection.com/2013/11/articles/consumer-privacy/european-commission-calls-for-data-transfer-reforms/>.

- insufficient accessibility to privacy policies of Safe Harbor companies is to the detriment of individuals whose personal data is being collected and processed, and may constitute a violation of the principle of notice. As a result, individuals whose data is being transferred from the EU may be unaware of their rights and the obligations to which a self-certified company is subjected (*the OAIC notes that for entities covered by the APPs (which require that such entities have a clear and accessible privacy policy), this criticism may not be relevant*)
- up to 10% of Safe-Harbor certified companies may not be living up to the requirements to post compliant privacy policies on their public websites (*presumably, if signed up to or caught under an Australian scheme, the OAIC anticipates that these companies may also fail to live up to the Australian scheme requirements*)
- recent statistics demonstrate false claims of Safe Harbour adherence - about 10% of companies claiming membership in the Safe Harbour are not listed by the Department of Commerce as current members
- the US Department of Commerce's reviews of Safe Harbor renewals tend to focus on the evaluation of formal requirements rather than investigations of actual practices.

In formulating a safe harbour scheme for Australia, consideration should be given to how these sorts of issues may be addressed.

Question 11-1: What, if any, provisions should the ALRC propose regarding a court's power to make costs orders?

The OAIC considers that other stakeholders have more expertise and experience to comment specifically on provisions relating to a court's power to make costs orders.

However, consistent with guiding principle 8 for this ALRC inquiry ('justice to protect privacy should be accessible'),[17] it is important that access to justice is taken into account in considering the development of any provisions regarding a court's power to make costs orders. In particular, the OAIC notes that the accessibility of the serious privacy invasion tort may be compromised by the potential for adverse costs orders against unsuccessful plaintiffs.

[17] See DP 80 at paragraphs [2.33]-[2.35].

Proposal 15-1: The ACMA should be empowered, where there has been a privacy complaint under a broadcasting code of practice and where the ACMA determines that a broadcaster's act or conduct is a serious invasion of the complainant's privacy, to make a declaration that the complainant is entitled to a specified amount of compensation. The ACMA should, in making such a determination, have regard to freedom of expression and the public interest.

A risk of the proposal to empower the ACMA to award compensation in certain situations is that it will introduce further fragmentation into privacy regulation and protections. In particular:

- this proposal would introduce a complaints model that is only available for a narrow subset of all serious privacy invasions (being those committed by broadcasters and which also breach a broadcasting code)
- for serious media invasions of privacy, this proposal would introduce a right to receive compensation for some privacy invasions (being those committed by broadcasters which are also a breach of a broadcasting code), while no similar right would be available for other media privacy invasions, such as those committed by the print and online media
- there would be fragmentation in terms of where individuals need to go to obtain a remedy for privacy breach, with affected individuals:
    - complaining to the OAIC in the case of interference with privacy
    - complaining to the ACMA for serious invasion of privacy by broadcasters
    - commencing court proceedings for serious privacy invasion in all other instances.

Further, while the ACMA is best placed to comment on the impact this new function will have on the ACMA's activities, the OAIC notes that Proposal 15-1 would confer on the ACMA a role of providing redress to affected individuals. The ACMA's submission in response to the ALRC's Issues Paper 43 stated 'Media and communications industry regulation is aimed at industry-wide practices, addressing systemic issues relating to privacy rather than providing redress for affected individuals.'[18]

The OAIC understands that a key reason behind this proposal is to provide individuals with an alternative to costly litigation.[19] Generally, the OAIC is supportive of measures that encourage the early resolution of disputes and provide increased access to justice for affected individuals. However, the OAIC believes this is best achieved by a complaints model that applies consistently to all serious invasions of privacy, rather than a complaint mechanism for a specific subset of cases.

---

[18] Australian Communications and Media Authority November 2013, *Submission by the Australian Communications and Media Authority to the Australian Law Reform Commission Inquiry into Serious Invasions of Privacy in the Digital Era – Issues Paper 43,* p 2, available at <www.alrc.gov.au/inquiries/invasions-privacy/submissions>.

[19] See DP 80 at paragraph [15.17].

Proposal 15-2: A new Australian Privacy Principle should be inserted into the Privacy Act 1988 (Cth) that would:

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

The OAIC does not support the introduction of the new Australian Privacy Principle (APP) proposed by the ALRC in Proposal 15-2.

First, the OAIC notes that the new APP would not apply to agencies. Almost all personal information held by an agency is held in a Commonwealth record. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the *Archives Act 1983*.

Second, the OAIC considers that the new APP is unnecessary in light of the existing requirements contained in the APPs in Schedule 1 of the Privacy Act. The OAIC considers that the existing APPs appropriately balance an individual's privacy interests with the interests of entities in carrying out their functions or activities (see the objects of the Privacy Act in s 2A).

The measures in APP 3 and APP 5 ensure that entities only collect information which they legitimately need, and allow an individual to make an informed decision about whether to provide their personal information to an APP entity. The measures in APP 6 and APP 11 provide limits on how collected information can be used and disclosed and how long it can be retained. For example, under the existing APPs, an APP entity:

- can only collect personal information where it is reasonably necessary for the entity's functions or activities (or, for an agency, also where it is directly related to the agency's functions or activities) (APP 3)
- must generally collect personal information directly from the individual concerned (APP 3.6)
- must take reasonable steps to notify or make an individual aware of certain matters in relation to the collection of personal information (APP 5)
- must only use or disclose personal information for the primary purpose for which it was collected, unless an exception applies (APP 6)
- if the entity is an organisation, must generally destroy or de-identify personal information when it can no longer use or disclose it for any authorised purpose (agencies must instead comply with the provisions of the *Archives Act 1983*) (APP 11).

In particular, under APP 11, if an individual were to request an organisation to destroy personal information which the entity holds about the individual because, for example,

the individual no longer wished to deal with that entity, then the organisation would be required to destroy or de-identify the information under APP 11, unless there remained a lawful purpose or requirement to retain the information. If the organisation failed to do so, the individual could lodge a complaint with the OAIC.

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 (and so therefore not required to destroy or de-identify it under APP 11), 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.

One option for addressing concerns about destruction or de-identification on request is for the OAIC to 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.[20]

Question 15-1: Should the new APP proposed in Proposal 15-2 also require an APP entity to take steps with regard to third parties with which it has shared the personal information? If so, what steps should be taken?

As outlined in response to Proposal 15-2, the OAIC does not support the introduction of a new APP relating to destruction of personal information upon request. However, in the event the new APP is introduced, the OAIC makes the following comments.

The OAIC considers that the burden that additional steps with respect to third parties would impose on APP entities outweighs the privacy benefits that those additional steps would create for an individual.

DP 80 canvasses the options of requiring an APP entity to notify the third parties with which it has shared the personal information of the individual's request for destruction, or alternatively, requiring the APP entity to notify the individual of the third parties with which it has shared the individual's personal information.

However, Proposal 15-2 does not seek to require the third party to destroy or de-identify personal information upon being informed by the APP entity of the individual's destruction or de-identification request. Similarly, while an individual could request a third party to destroy or de-identify the personal information if notified by the APP entity of those third parties, the third party would have no obligation to do so where the information was not originally provided by the individual.

There are already a number of notification requirements on APP entities in relation to the disclosure of personal information, including in APP 1 (privacy policy requirements), APP

[20] Section 28 of the *Privacy Act 1988* confers various guidance related functions on the Australian Information Commissioner.

5 (notice at collection) and APP 7 (direct marketing). The OAIC considers that these obligations on APP entities are sufficient for enabling an individual to understand the third parties to which the original APP entity discloses their personal information.

Question 15-2: Should a regulator be empowered to order an organisation to remove privacy information about an individual, whether provided by that individual or a third party, from a website or online service controlled by that organisation where:

- **an individual makes a request to the regulator to exercise its power;**
- **the individual has made a request to the organisation and the request has been rejected or has not been responded to within a reasonable time; and**
- **the regulator considers that the posting of the information constitutes a serious invasion of privacy having regard to the freedom of expression and other public interests?**

Take-down powers may be an effective tool in cases of serious invasions of privacy (such as revenge porn, doxing and harassment).

The OAIC would be generally supportive of such a take-down power, to the extent it would achieve resolution of serious invasions of privacy in a fast, informal and low-cost way.

Clarification required

The OAIC suggests that the ALRC may need to further consider how such orders would work in practice. For example:

(a) The question indicates that the ALRC is proposing that orders be made against organisations. Which organisations are intended to be covered? For example, will the power be limited to 'organisations' as defined under the Privacy Act, or will it include government agencies and small business operators? The OAIC also suggests that consideration be given to whether individuals acting in their personal capacity should be covered (see (b) below).

(b) What is meant by 'controlled' in this question? For example, a website or online service may be 'controlled' by an individual, such as a blogger, that is not an 'internet intermediary' as defined by the ALRC in Chapter 10 of DP 80.

(c) What is meant by 'privacy information'? For example, is this term intended to be wider in scope than the definition of 'personal information' in the Privacy Act and, if yes, what additional categories of information will this term cover?

Design for the power

To be effective, any take-down mechanism will need to be able to be applied quickly, and the mechanism's procedural requirements should reflect this. It will be important that

the mechanism balances administrative justice (eg rights of appeal, timely review of decision) with effective resolution of serious invasions of privacy.

Further, unless the tort proposed by the ALRC is enacted, consideration will need to be given to the elements that make up a serious invasion of privacy.

If the OAIC were the chosen regulator, the Australian Information Commissioner could develop guidelines about what acts and practices may constitute serious invasions of privacy. The Commissioner is empowered to do so under guidance related functions in s 28 of the Privacy Act (however the OAIC notes that any such guidelines would not be a binding legislative instrument).

The Commissioner may also issue guidance for individuals to assist them with determining whether their grievance is one that satisfies any criteria for submitting a takedown request. The Commissioner already does this for general privacy complaints.[21]

Determining the appropriate regulator

The OAIC notes its expertise and experience in privacy complaint handling. To some extent, a takedown mechanism as proposed in this question mirrors the OAIC's current complaint handling process. Further, a take-down power would be similar to the OAIC's other powers, such as to accept enforceable undertakings and make determinations (including as part of resolving a complaint). For this reason, the OAIC may be the appropriate regulator to issue a take-down order.

A take-down power would create additional workload for the relevant regulator and would need to be resourced accordingly.

Enforcement difficulties

The OAIC notes that take-down orders will be difficult to enforce where the wrongdoer is located outside of Australia, on both a jurisdictional and practical basis. These difficulties should be taken into account in the design of any take-down mechanism.

Proposal 15-3: The *Privacy Act 1988* (Cth) should be amended to confer the following additional functions on the Australian Information Commissioner in relation to court proceedings relating to interferences with the privacy of an individual:

- **assisting the court as amicus curiae, where the Commissioner considers it appropriate with the leave of the court; and**
- **intervening in court proceedings, where the Commissioner considers it appropriate, with the leave of the court.**

The OAIC understands that Proposal 15-3 is suggesting that the Australian Information Commissioner have the functions of appearing as an amicus curiae or intervener in court proceedings relating to interferences with privacy under the Privacy Act as defined in s 13 of the Privacy Act (as opposed to serious privacy invasion proceedings). The OAIC

[21] Office of the Australian Information Commissioner, *Privacy complaints*, available at <www.oaic.gov.au/privacy/privacy-complaints>.

supports this proposal in principle. The OAIC notes, however, that at present there are very few court proceedings relating to interference with privacy, and few that arise where the OAIC is not an existing party. One example where the opportunity could arise is injunction proceedings under s 98 of the Privacy Act, although this section has rarely been used since its enactment.[22]

The OAIC has previously suggested conferring both amicus curiae and intervener roles on the Australian Information Commissioner in relation to court proceedings for serious invasion of privacy (as opposed to privacy interference proceedings).[23] The OAIC continues to support the conferral of these roles in the context of the complaints model for serious privacy invasion being adopted.

However, if, as envisaged by the proposals in DP 80, the OAIC is to have no other role in relation to dealing with allegations of serious privacy invasion, the OAIC questions whether it is appropriate for the Australian Information Commissioner to be granted amicus curiae and intervener functions for court proceedings relating to serious privacy invasion.

[22] The OAIC is only aware of two instances in which s 98 has been successfully used: *Smallbone v New South Wales Bar Association* [2011] FCA 1145 and *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* [2004] FCA 637.

[23] OAIC December 2013, *Serious invasions of privacy in the digital era – submission to the Australian Law Reform Commission*, response to Question 20; OAIC November 2011, *Issues Paper – A Commonwealth statutory cause of action for serious invasion of privacy – Submission to the Attorney-General's Department*, paragraphs [50]-[52].