Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

12 May 2014

The Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001
privacy@alrc.gov.au

Dear Executive Director,

Re: Discussion Paper 80: Serious Invasions of Privacy

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

We attach our submission relating to the above Discussion Paper.

Thank you for your consideration.

Yours sincerely

Associate Professor David Lindsay
Ph: (03) 9905 5547
david.lindsay@privacy.org.au
david.lindsay@monash.edu

Peter A. Clarke
Barrister
Isaacs Chambers
555 Lonsdale Street, Melbourne
Ph: (03) 9225 8751
papclarke@optusnet.com.au

for the board of the Australian Privacy Foundation.

Australian Privacy Foundation

ALRC Discussion Paper 80: Serious Invasions of Privacy

12 May 2014

This document presents APF's Submission in relation to the Discussion Paper.

4. A statutory tort for serious invasion of privacy

Proposals 4-1 & 4-2

The Australian Privacy Foundation (the "APF") **strongly supports a statutory right of privacy and a viable cause of action available to individuals to enforce that right.** To that extent the APF endorses the Commission's proposals to establish a cause of action. While the nomenclature is not a matter of significant moment to the APF it is appropriate to describe the action as an action in tort[1]. In recommending a cause of action for breach of privacy each of the Australian Law Reform ALRC (the "ALRC"), the Victorian Law Reform Commission ("VLRC") and the New South Wales Law Reform Commission ("NSWLRC") have proposed different models.

The overall and overriding objective of the APF is that any cause of action must be robust, flexible, adaptable and have broad coverage with only very limited and specific exceptions (by means of defences), and be reasonably accessible to individuals in giving them an enforceable right for breaches of their privacy. **The threshold for commencing an action should not be high.** The action should be sufficiently flexible to allow the tort to adapt with changes in technology and be responsive to societal mores. **The remedies must be robust, diverse and responsive to the ills caused by breaches, including damages, apologies, correction, declaratory and injunctive relief.** There should be scope to award significant damages, both general and special. Courts are not generous in the award of damages overall, and general damages specifically. A court should have the discretion to award both aggravated and exemplary damages where the circumstances justify such an award. The cause of action must permit defences which represent relevant competing interests.

Care must be taken that the elements of the tort do not, by their architecture unduly constrict its overall operation; for example constraints that may encompass the operation of the "reasonable expectation" element. If this element of the tort is, overall, so difficult to establish it will rarely be used and thereby risks continuing the current problems whereby many serious intrusions are not effectively remedied by legal means. As a consequence the perception will be that those responsible will be seen to "get away with it" and to repeat intrusions with impunity. This may have the perverse effect of ratcheting down the level of protection one might "reasonably expect", thus making use of the tort harder over time. This potential "design flaw" of the tort calls for extra efforts to ensure that other potential obstacles to its use are minimised, so people may "reasonably expect" protection and be able to avail themselves of it.

The existing tort in the United States and that which has developed in Canada and New Zealand is structured in a manner consistent with common law intentional torts. Defendants are able to avail themselves of specific defences. The United Kingdom ("UK") privacy jurisprudence, by comparison, is grounded in equity and the court must undertake a balancing exercise between the rights set out in Articles 8 and 10 of the *Human Rights* Act 1998 (UK). The underlying principles of each head of action differ in significant ways. It is an important distinction. The ALRC's proposed cause of action is a hybrid of an intentional tort, as set out in the proposed first four elements, and a balancing exercise as undertaken by UK courts, as reflected in the fifth element.

The APF believes that the most effective structure of a cause of action is that which is consistent with an intentional tort; consisting of elements that a plaintiff must satisfy with countervailing defences available to any putative defendant. There should be no requirement for the court to undertake a balancing exercise as an essential element in determining whether the plaintiff can, on his or her own case, succeed or not.

Proposal 4-2
The APF submits that **the cause of action for a 'serious invasion of privacy' should additionally be described as an 'interference with privacy' for the purposes of the *Privacy Act 1988* (Cth).** This is discussed further under 'Forums, Limitations and Other Matters' and 'New Regulatory Measures' below.

Elements of the Tort

5. Two Types of Invasion and Fault

Proposal 5-1: First element. intrusion upon seclusion or private affairs, misuse or disclosure of private information

In general, the APF supports the scope of the first element of the ALRC's proposed cause of action, that the focus of the tort should be upon the intrusion into a plaintiff's seclusion or private affairs (including by unlawful surveillance) and/or the misuse or disclosure of private information about the plaintiff.

Proposal 5-2: Second element. The tort should be confined to intentional or reckless invasions of privacy and not extend to negligent invasions.

Regarding the second element of the proposed tort, the APF considers that **there is no sound legal or policy basis for limiting the scope of the action to either intentional or reckless acts rather than incorporating negligent acts.** Accordingly, the APF considers that, in this respect, the ALRC's proposal is unnecessarily restrictive. The ALRC itself acknowledges that restricting the action to intentional or reckless acts will mean there are cases where individuals will have no remedy. For those who suffer harm as a result of privacy invasions, it is little consolation that the tort will reduce rather than remove a recognised gap in the law.

It is poor policy for the ALRC to claim that if a plaintiff suffers loss as a consequence of negligent acts which breach his or her privacy that the appropriate recourse should be to make a claim in negligence[2] or contract.[3] This would represent a cumbersome and unnecessary segmentation of what should be a seamless and broad protection, aimed at redressing a recognised gap in the law. More importantly, breaches of privacy involve discrete issues which are not suited to a claim in negligence or contract. As proposed, a person who has a reasonable expectation of privacy may sustain an action where a putative defendant intrudes upon his or her seclusion and causes him or her significant emotional distress. In these circumstances, whether the means by which the intrusion took place was reckless or merely negligent will be decisive in determining whether the plaintiff has a claim. As the harm sought to be addressed by the tort may be the same, this appears to be an arcane distinction. Given the threshold issue (whether the act is intentional, reckless or negligent) may be critical in determining whether a person has a claim or not, it will likely lead to significant and time-consuming argument as to the nature of reckless acts rather than those of a negligent variety in the discrete area of privacy jurisprudence.

It is important to stress that the action proposed by the ALRC will be entirely based on statute. Consequently, the stated policy concerns, such as that emotional distress is not generally compensable for negligent acts are otiose. To assert that the policy of the common law is not to award damages for emotional distress that is negligently inflicted is to answer the wrong question. **The APF submits that the parameters of the proposed tort should be based on the correct**

policy question, namely what elements of the cause of action are best adapted to address the harms arising from serious invasions of privacy?

Similarly, there is no persuasive legal argument that damages in a statutory cause of action must be confined to general damages for emotional distress, rather than special damages including economic loss. That emotional distress may be a "key type of harm"[4], which is beyond dispute, does not mean it is the only type of harm suffered. Nor does it mean that it should be the only type of harm that should be compensated by a statute aimed at redressing serious harms to privacy.

The ALRC's conclusion that having both intentional/reckless and negligent acts encompassed as elements in a cause of action would undermine the coherence in the law is not persuasive. That the legislature may give an individual the right to recover general damages for negligent acts arising out of a privacy breach will not, as a matter of law, alter the common law position regarding other forms of negligence. The nature of the breach is distinct and the facts are commonly, if not invariably, different from those involving other forms of negligence. A statutory cause of action involving breach of privacy is discrete and stands alone, being designed to address specific forms of harm. Moreover, the ALRC does not rely upon evidence to demonstrate that recognising a cause of action for negligent invasions of privacy would influence, undermine or detract from the operation and development of other discrete common law causes of action.

The ALRC's suggestion that extending liability to negligence might lead to excessive self censorship and too great a chilling effect on every day activities[5] is more consistent with assertion than analysis and barely rises above speculation. **Concerns that negligent actions may inhibit expression, chill free speech and expose those to liability for unintentionally invading someone's privacy should be obviated by a robust public interest defence which adequately protects freedom of expression.** Having a broader scope for actionable conduct with a proper, carefully defined, robust defence would avoid the need for arcane and overly-complex arguments as to whether conduct is reckless rather than negligent.

Proposals 5-3 & 5.4: Effect of an apology relating to invasion of privacy.

The APF agrees that an apology or correction of published material by a defendant should not be treated in evidence as an admission of fault. The APF further submits that it is unnecessary to provide for the elimination of causes of action already in existence. The existence of the tort is to address the specific goal of filling a gap in the law in this particular area. The concern about an overlap is, in any case, more abstract than real and a matter that does not require legislative action.

6. A Reasonable Expectation of Privacy

Proposal 6-2: Third element. The tort should be only be actionable where the plaintiff has reasonable expectation of privacy.

The third element of the tort, the requirement that a person in the position of the plaintiff must have had a reasonable expectation of privacy in all of the circumstances is generally consistent with the development of the tort in other jurisdictions and the development of the equitable cause of action in the UK. As a general principle the APF supports having a non exhaustive, non binding, list of factors relevant in the consideration of a reasonable expectation of privacy, provided its operation does not extend, in law or practice, to limiting the factors parties may rely upon, those which the courts should consider and the weight that must be given to each, all or none of the factors in any particular case. Courts should have the broadest discretion as to what they should or should not consider. In this respect, the law should be allowed to develop incrementally and not within rigid structures.

However, as noted in the early part of this submission above, there is potential for intrusive practices to become entrenched if not successfully challenged, and to the extent that this becomes popular knowledge and industry practice, to inform and lower "reasonable expectations". If this element is adopted *and* the tort turns out to be difficult to establish and rarely used so that few if any successful actions occur, **there is potential for a downward ratchet effect: the lack of a practical remedy enables continuation of an intrusive practice without restraint, which practice reduces the level of protection that would be "reasonably expected", which in turn reduces the scope of the tort over time.** This is of particular concern in the fast-moving online environment, when key global actors such as Facebook and Google's approach is the antithesis of complying with Privacy Principles (or the precautionary principle), preferring a contrary mindset of "move fast and break things" and "ask forgiveness, not permission". These models encourage projecting privacy risk onto others speculatively, and iteratively assessing whether any response is ultimately adverse enough to warrant modifying the practice. Over time, if not adequately addressed, they may erode "reasonable expectations". **If such a requirement is included in the elements of the tort, to avoid potential for difficulties in its use to feed back into a lack of restraining effect on intrusions leading to reduced expectations (and thus standards) of protection, it is critical to minimise other obstacles to use of the tort, and support the most robust and effective legal and procedural model.**

Proposal 6-2: Considerations relevant in determining whether a person has a reasonable expectation of privacy

The APF considers that there is little utility in the factor set out in Proposal 6-2(i); the extent to which the plaintiff has manifested a desire not to have his or her privacy invaded. It is poor public policy for a person to need to express a desire not to be the subject of a tortious wrong. Even as merely one factor, amongst many, in a non exhaustive list does not seem to be appropriate. At a practical level how should such desire be manifested? Such a factor is likely to be used by defendants who may use the lack of a demonstrated, overt desire as being a factor to be taken into account against a plaintiff. Similarly great care should be given in taking into account the age[6] and occupation[7] of a party as being any part of a relevant factor. Such an approach has the potential to arbitrarily segment the operation of the law. Even the slightest possibility that the law may apply differently depending on age, educational standards, profession of the plaintiff should generally be avoided. In particular, reference to occupation at Proposal 6-2 (g) could conceivably be used to establish some form of "public figure" consideration which may warrant less protection being afforded to certain individuals. It is too broad and vague. Other factors are more reasonable, such as where the intrusion occurred[8], the sensitivity of the information involved[9], and the purpose of the misuse.

7. Seriousness and Proof of Damage

Proposal 7-1: Fourth Element. The tort is only available where the invasion of privacy is 'serious'.

The fourth element of the tort is, as a threshold issue, both unnecessary and arbitrary. If the cause of action is structured as an intentional tort, as the cause of action appears to be, damage should be presumed. The remedy, whether in the form of injunctive relief, damages or other relief, will (or should) reflect the seriousness of the breach. To that extent establishing a threshold of 'serious in all the circumstances' is unnecessary. Similarly, delineating conduct as highly offensive rather than merely offensive is also unnecessary. Offensive conduct is a sufficiently high threshold if there is to be one. **Furthermore, the distinction between "highly offensive" and "offensive" at law and in practice is not entirely clear.** Clearly the former behaviour is worse than the latter. Beyond that the ALRC provides little analysis or guidance. Such vague and uncertain distinctions

[6] Paragraph 6.45

[7] Ibid 6.46

will result in a vigorous dispute between plaintiffs and defendants along the wide and blurred fault line between 'offensive' and 'highly offensive' conduct. Court resources would be better spent on more substantial issues. The egregiousness of the conduct, if found to constitute a breach, should be reflected in the scope and, where appropriate, quantum of damages.

8. Balancing Privacy with Other Interests

Proposal 8-1: Fifth Element. The balancing exercise and no public interest defence.

The APF submits that there is little utility in incorporating a balancing exercise of the plaintiff's privacy interest against freedom of expression or other broader public interest, the fifth element of the proposed cause of action. In the APF's view, ideally the issues of freedom of expression and other legitimate defences should be discrete defences. The balancing of interests proposed by the ALRC is more consistent with the approach taken by the UK courts when considering Articles 8 and 10 of the *Human Rights* Act 1998 (UK) as they are required to do. That exercise is done as part of an equitable cause of action, the misuse of private information. That is a separate and distinct cause of action to that of the statutory tort proposed by the ALRC, which incorporates an action against intrusion.

The APF does not accept the assertion that it is widely accepted that the public interest must be considered at some stage in an action for breach of privacy.[10] That presupposes that public interest considerations apply as a matter of course and all privacy actions follow a similar pattern and will continue to do so.

In practice, in tortious claims it is more appropriate and efficacious for a defendant to plead defences of his/her/its own choice, facts and law permitting. Defendants may not necessarily wish to agitate any form of 'public interest' defences, as should be their right. There may be good legal, tactical and practical reasons to avoid agitating some defences, which may include public interest related defences even if the facts permit it. If a defendant does not wish to rely upon a public interest defence, for example, simply alleging the act did not take place and nothing further, and the plaintiff claims there is no public interest issue, then the mandated exercise of taking public interest into account as part of the cause of action will be artificial, unnecessarily time consuming and costly. Having the two reluctant parties having to address an issue neither believes applies is the antithesis of modern civil procedure and case management.

The APF acknowledges that there may be some potential dangers with a broadly-framed 'public interest' defence, associated in part with the terminology. In particular, the APF believes that the protection of privacy is a public interest as well as a private interest, so use of "public interest" (in opposition to the interest in protecting privacy) can potentially be misleading. Moreover, the protection of privacy (and related rights and interests, such as confidentiality and information security) may support other public interests including, on occasion, the right to freedom of expression. Any reference to the "broader public interest" in the context of this tort should therefore include some acknowledgement of privacy's key role in support of other public interests, and not imply automatic incompatibility with or hostility to privacy and related values. This could, for example, be achieved through appropriate use of interpretative material, such as an objects clause in the proposed legislation, or appropriate qualifications in the explanatory memorandum.

On the broader point, the APF submits that there is no evidence for concluding that having public interest as a defence, rather than an element of the cause of action, would prolong the length of time of an unmeritorious claim. It is questionable whether the ALRC's proposed fifth element would work to limit unmeritorious actions in the context of the civil procedure rules and legislation in the state jurisdictions and at the Commonwealth level. Public interest considerations would invariably involve considerations of both fact and law. They are certainly not given to resolution at the interlocutory stage, whether by way of strike out or summary judgment applications. It is unlikely that even with a weak claim by a plaintiff that upon the consideration of public interest issues a court would terminate a trial prior to the defendant's case opening and evidence being presented. In practice, facts are rarely tidy.

Moreover, the relevant evidence to be taken into consideration regarding the fifth element is unlikely to arise solely from the plaintiff's camp. There may be evidence the defence may be able to lead which will assist the court in properly considering the public interest issues. In fact, the defendant will usually be best placed to give evidence on whether or not the conduct is justified as a matter of public interest. In the normal course, the defendant's witnesses give their evidence in chief upon the conclusion of the plaintiff's case. It is artificial to assume that a court will refrain from considering all the evidence before making findings of fact and law and final orders. Further, the ALRC's argument on this point is somewhat divorced from reality in that courts in Australia are normally very reluctant to make final orders until all the admissible evidence has been led. Given the ALRC does not suggest changing the rules of civil procedure there is no basis to assert that having public interest as a defence will lengthen a trial.

That the ALRC refers to and, presumably, relies upon the balancing exercise taking place in the UK is not persuasive.[11] As submitted earlier, equity is not tort. In any event the balancing exercise undertaken in the UK is necessitated by the operation of the *Human Rights* Act 1998 (UK). There is no such equivalent legislation in Australia or in contemplation. Claiming that leaving public interest as a defence risks a plaintiff more easily using court proceedings to stifle legitimate exposure of matters of public concern is more assertion than conclusion based on facts capable of independent analysis. Abuse of process is not a new development in litigation and reforms of the civil procedure rules throughout Australia have enhanced the power of courts to deal with such mischief.

Further there are fact situations where public interest defences are not relevant. For example it does not follow that a privacy action will necessarily, or even often, involve freedom of expression issues. Breaches of privacy, much like defamation proceedings, do not invariably involve the media. The facts can, and often are, more prosaic and do not throw up significant public interest issues even if they involve an invasion of privacy.

Some of the proposed public interest factors in Proposal 8-2 are potentially not appropriate at all or far too broad. In this respect, we offer general support to observations we understand to be made by the Cyberspace Law and Policy Community (the “CLPC”) raising concerns about the excessive generality, scope and difficulty in definition of matters particularly around administration of government, the economic wellbeing of the country, and the defence of “legal authority”. These are not appropriate or appropriately narrowly limited, and so could seriously undermine the effectiveness of the proposed cause of action.

9. Forums, Limitations and Other Matters

Proposal 9-1

The ALRC proposes that federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy under the proposed new Act.

The implication of the APF's submissions on Proposals 4-2 and 15 is that the Privacy Commissioner/AIC will also have jurisdiction, by virtue of the action also being an 'interference with privacy' for the purposes of the Privacy Act.

The APF supports the ALRC proposal that Federal, State and Territory courts should have jurisdiction to hear a serious invasion of privacy action. The inclusion of lower levels of State and Territory courts is, in particular, supported because, as PIAC and others have submitted, '[a]ccessibility is a key factor in considering which forum is appropriate …'. The APF supports complainants/plaintiffs having the option to take actions for interferences with privacy to the Courts, not only to the Privacy Commissioner, *a fortiori* in the case of a 'serious invasion of privacy'.

However, **the APF considers there are very strong reasons for providing the option to complainants/plaintiffs to take a 'serious invasion of privacy' complaint to the Privacy Commissioner.** The APF also submits that there are no significant impediments in law or policy to this approach.

The APF submits that the ALRC's reasons in [9.30]-[9.32] of the Discussion Paper for rejecting complaints of a 'serious interference with privacy' being able to be brought before the Privacy Commissioner/AIC are not convincing, and should be reconsidered. The reasons for reconsideration are as follows:

(i) The mechanism of making a 'serious invasion of privacy' also an 'interference with privacy' for the purposes of the Privacy Act avoids any problem of vesting of judicial powers (a problem identified in vesting jurisdiction in Commonwealth tribunals).

(ii) This mechanism is a familiar part of federal legislative techniques, used in such areas as TFNs, and other examples in section 13 of the Privacy Act. It was used most recently in the *Privacy Amendment (Privacy Alerts) Bill* 2013, Schedule 1, item 3, which proposed insertion of a new section 13(4A) in the Privacy Act, to make contraventions of a data breach notification requirement also an interference with privacy.

(iii) Some complaints over which the Privacy Commissioner already has jurisdiction under the APPs may already constitute 'serious invasions of privacy'. One example is APP 3.5, which prevents collection of personal information by unfair means. Various types of intrusive or deceptive information collection can also constitute the intrusion tort (Proposal 5-1(a)). Complaints under APP 3.5 could involve the most difficult issues of intrusive media conduct, and require balancing of privacy and free speech considerations. Privacy Commissioners in other jurisdictions, such as Hong Kong,[12] deal competently with such issues. If the Privacy Commissioner/AIC is going to have

[12] Hong Kong's Privacy Commissioner for Personal Data interpreted 'fair' to include 'not intrusive' in two 2012 complaints. Each complaint concerned 'paparazzi' style photo-journalism using systematic surveillance and telescopic lens photography to take clandestine photographs of TV personalities within their private residences, over a period of three to four days. The Commissioner found both respondents in breach of DPP 1(2), and served enforcement notices directing the magazines to remedy their contraventions and the matters occasioning them. On appeal, the Administrative Appeals Board (AAB) dismissed all five grounds of appeal by each of respondents. The media respondents raised public interest arguments based on *Campbell v MGN* but that decision was distinguished on various grounds. In Hong Kong, 'public figures' are therefore able to protect some aspects of their private lives, through use of the privacy Ordinance. See *Face Magazine Ltd and the PCPD*, [2012] HKPCPDAAB 5; *Sudden Weekly Ltd and the PCPD*, [2012] HKPCPDAAB 6. The appeal

jurisdiction over the substance of *some* 'serious invasions of privacy', it would seem sensible for the Commissioner to be an alternative means of dispute resolution for *all* 'serious invasions of privacy', given that there are no constitutional impediments to this being achieved. It would also have significant advantages.

(iv) Referring to the Privacy Commissioner/AIC, the ALRC says that 'In the absence of significant reform, the remits of these administrative bodies are typically restricted to information privacy, and to particular entities such as government agencies or large businesses' [9.31]. This is not a convincing argument. First, the intrusion tort will often be about intrusive collection of information, and the second branch of the proposed tort is solely about 'private information', so it is likely that most 'serious invasions of privacy' will in fact be about 'information privacy'. There is no obvious reason why a Privacy Commissioner would not have the skill set to deal with balancing privacy interests in relation to bodily privacy, communications privacy or spatial privacy, particularly because so many of those issues have significant overlaps with information privacy.

(v) The ALRC's reference to 'large businesses' implies that the Privacy Commissioner/AIC should have no role in relation to 'small business'. That exemption in the Australian federal law does not currently apply in the most serious instances of privacy interferences, where personal information is sold, bought or traded, so it is not anomalous if it does not apply in what are defined as 'serious invasions of privacy'. The Australian law is peculiar (along with Japan's law) in having a 'small business' exemption. All other overseas data protection authorities deal with complaints against small businesses. The ALRC has previously recommended abolition of the 'small business' exemption in the ALRC Report *For Your Information*.

(vi) The ALRC also implies that the Privacy Commissioner/AIC should not investigate complaints about individuals. While the Privacy Act section 16 does exclude 'personal, family or household affairs' from the scope of the APPs, it does not exclude investigation of complaints against individuals in other contexts. There is no good policy reason why 'serious invasions of privacy' by individuals should not be investigated by the Privacy Commissioner/AIC. Many appropriate defences will apply, without need for any *a priori* exclusion of 'personal, family or household affairs'. In fact, it is in that context that many of the most egregious invasions of privacy occur, and where other individuals with few resources to run expensive litigation need the option of a remedy under the Privacy Act.

In short, **the ALRC has not identified compelling policy reasons for excluding the Privacy Commissioner/AIC from dealing with 'serious invasions of privacy'.**

The action would operate as an 'interference with privacy' in the Privacy Act as follows:

1. The existing wording of the *Privacy Act* is sufficiently flexible for the Privacy Commissioner to hear complaints about 'serious invasions of privacy' against all relevant parties, and to make such orders as are provided for by the Privacy Act. It does not seem that any further changes to the Act would be necessary, except possibly as noted in (4) below.

2. Appeals against determinations by the Commissioner could then be made to the AAT, and further appeals to the federal courts where necessary. The Privacy Act already provides in section 96(1)(c) for appeals concerning acts or practices of private sector bodies to go to the AAT in relation to the APPs, so there is now nothing unusual about this. As the ALRC notes, AAT appeals will still constitute 'review of decisions made by administrative bodies' [9.29], namely the Privacy Commissioner.

3. The proposed action for 'serious invasions of privacy' is not subject to exemptions for particular types of organisations, acts or practices, but instead is subject to various

Consistent with this, the restrictions imposed by the definition of 'acts and practices' in section 7 of the Privacy Act, or sections 7B and 7C, should not apply to how it is defined as an 'interference with privacy'. The APF therefore submits that a new sub-section 13(6) should be added to the *Privacy Act 1988* (Cth): '(6) A serious invasion of privacy under the [title of new Commonwealth Act] is an interference with the privacy of an individual.'[13]

4. Despite the previous comment, it may reasonably be considered that it is not appropriate for the Privacy Commissioner to investigate the conduct of certain parties, such as some of those referred to in section 7(1)(a) and (b) of the Privacy Act. A new provision excluding those parties may be required. Nevertheless, complainants against such parties would still have the option of taking the matter before a court.

As well as there being no obvious impediments to the Privacy Commissioner/AIC having a new function of investigating complaints of 'serious invasion of privacy', there are numerous and considerable advantages, including the following:

(i) The accessibility advantages of being able to complain to the Privacy Commissioner are significant, and comparable with or better than most advantages of the lower levels of State or Territory courts. There are no court costs, or costs awarded against parties, but there is a high likelihood of many complaints being dismissed on the basis that the Commissioner considers there is not a 'serious invasion of privacy' (interference with privacy), or that the respondent has dealt with it adequately. Lower-level courts have more de-centralised physical distribution, and the advantage that plaintiffs usually have their 'day in court'. Each approach has different advantages in terms of accessibility, and the best result for complaints/plaintiffs is to have a choice.

(ii) The Privacy Commissioner is likely to have more experience and expertise in analysing the complex issues involved in a 'serious invasion of privacy' than will be the case for a lower level of State or Territory court.

(iii) Until there are significant decisions by higher level courts, published decisions by the Privacy Commissioner and (on appeal) the AAT are likely to be more numerous, and to give all relevant parties some guidance on how the new action is being interpreted. Assuming these decisions are of good quality, this is also likely to encourage more consistent decisions.

(iv) The Privacy Act provides a very flexible range of remedies (particularly after the new amendments), including extensive resort to mediated settlements and enforceable undertakings.

(v) It will be undesirable if the Privacy Commissioner/AIC appears to be excluded from consideration of *serious* invasions of privacy,[14] with the risk that the APPs and the Privacy Commissioner comes to be perceived as only relevant to *non-serious* invasions of privacy. This would be likely to be detrimental to compliance with the Privacy Act. In addition, it would be detrimental to the professionalism and expertise of the OAIC if its Commissioners and staff consider that they have no role to play (and therefore no need to acquire expertise) in relation to what are perceived to be the most serious privacy invasions, and the public interest and other considerations required to resolve them.

The APF therefore submits that a new sub-section 13(6) should be added to the *Privacy Act 1988* (Cth): '(6) A serious invasion of privacy under the [title of new Commonwealth Act] is an interference with the privacy of an individual,' together with such limited consequential

[13] The wording cannot say 'An act or practice is an interference with the privacy of an individual if the act or practice is a serious invasion of privacy under the [title of new Commonwealth Act]', like the rest of s13, without the undesirable effect of bringing in most of the exemptions from the Privacy Act

changes (if any) as are necessary to make the Privacy Act consistent with the new statutory action and the [title of new Commonwealth Act].

12, Breach of Confidence Actions for Misuse of Private Information

Proposal 12-1

The APF agrees with the ALRC that **there is a case for clarifying the availability of compensation for emotional distress in actions for breach of confidence**. Although the Victorian Court of Appeal in *Giller v Procopets* (2008) 24 VR 1 held that equitable compensation could be recovered for emotional distress in an action for breach of confidence, the position remains unnecessarily complex and uncertain. As emotional distress is often the main harm arising from a breach of confidence relating to personal or private confidential information, the availability of compensation for this harm is necessary to ensure that complainants are entitled to a suitable remedy.

The ALRC proposes that this reform should only be introduced if the proposal for introducing a statutory tort for serious invasion of privacy is not accepted.

Given the unsatisfactory lack of certainty in this area, however, the APF considers **that there may be a case for clarifying the law even if a statutory tort were to be introduced**. In this, the APF is not as concerned as the ALRC by the potential availability of more than one cause of action arising from the same set of facts. It may be, for example, that a breach of confidence involves both a misuse of personal information and an unauthorised use or disclosure of other information, such as commercial information. If a statutory tort were introduced, a complainant seeking compensation would still need to bring an action for breach of confidence in relation to the non-personal information. Although there may be an overlap between the statutory tort and the action for breach of confidence in relation to the misuse of personal information, the courts have well-established mechanisms for preventing double compensation.

The ALRC proposes that the desired statutory clarification should be confined to actions for breach of confidence that concern a serious invasion of privacy by the misuse, publication or disclosure of personal information.

The APF considers that **distinguishing actions for breach of confidence that involve personal information from those which do not risks introducing unnecessary complexity**. The introduction of a statutory clarification ensuring the availability of compensation for emotional distress in actions for breach of confidence would seem sufficient to achieve the desired objectives, given that courts can, in their discretion, be trusted to confine such awards to appropriate cases.

Proposal 12-2

The ALRC proposes statutory amendments providing that courts must have particular regard to freedom of expression and other countervailing public interests in considering whether to grant a pre-trial injunction to restrain publication of private information.

The APF agrees that courts hearing interlocutory applications must exercise caution where the application seeks prior restraint of publication, a position endorsed by Gleeson CJ and Crennan J in *ABC v O'Neill* (2006) 227 CLR 57.

The ALRC's proposal raises broader concerns than the relative weight to be given by courts to the public interest in freedom of political communication (and more broadly expression) in determining the balance of convenience in interlocutory applications in breach of confidence actions. There remains uncertainty about the extent to which public policy considerations can properly be taken into account by courts in considering the balance of convenience, some of which arises from the judgments in *ABC v O'Neill.* In that case, while the majority of the High Court rejected the application of 'special' principles to the award of interlocutory injunctions, the public interest in freedom of

taken into account, and the weight to be given to freedom of expression in the balance of convenience, is considered necessary, then there is a case for extending this beyond actions for breach of confidence. In any event, **if statutory amendments are considered necessary to ensure that the public interest in freedom of expression is properly taken into account in interlocutory applications to restrain publication of private information, the APF considers that the public interest in maintaining privacy must be given equal weight**. This is evident from the equal weight given to Articles 8 and 10 of the European Convention on Human Rights as part of the balancing exercise undertaken as part of the expanded action for breach of confidence under UK law (see, for example, the recent judgment in *Weller v Associated Newspapers* [2014] EWHC 1163 (QB)). On this point, the APF considers it is important to recognise that privacy, and the closely related concepts of 'personal information security' and 'confidentiality of personal communication', are just as much matters in which there is a public interest as, for example, freedom of expression. Moreover, privacy and related rights are, in many cases, the foundation of other rights. For instance, freedom of expression, freedom of association and freedom of religion may all require protection of privacy, personal information security and confidentiality for their full exercise. Consequently, proposals for expressly recognising public interest considerations in the context of actions for breach of confidence must also incorporate explicit recognition of the essential public interest character of privacy and related rights, including their central role in supporting other rights and freedoms,

Furthermore, **the APF disagrees with the ALRC's contention that different considerations should be applied to actions for breach of confidence aimed at protecting private information than apply to actions for protecting other confidential information** (DP, para [12.49]), as the public interest in protecting privacy is not a lesser interest than the public interest in protecting confidentiality. **Privileging 'commercial' information over 'personal' information that does not have a readily discernable commercial value (eg doesn't relate to a celebrity) also seems to be antithetical to the ALRC's proposal for introducing a cause of action regarding invasion of privacy**. It would, for example, perpetuate the problems evident in the *Douglas v Hello!* Litigation, where public figures are able to assert that information about themselves has a commercial value and thus can use confidentiality law to gain protection that may be unavailable to complainants who are not public figures or celebrities. Moreover, those who are not public figures or celebrities may find disregard of their privacy more distressing, as they are not inured to life under the spotlight.

The public interest considerations taken into account by courts exercising the balance of convenience in applications for interlocutory injunctions is conceptually distinct from the availability of, and the scope of, a public interest defence to actions for breach of confidence. The APF considers that Australian courts have adopted an unduly narrow approach to the public interest defence in the context of actions for breach of confidence, effectively ruling out considerations relating to the broader public interest in freedom of expression**. Just as there is a case for a public interest defence to a statutory action for serious invasion of privacy, there is a case for a public interest defence to actions for breach of confidence. There is no case, however, for specifically confining the defence to actions for protecting private information, as the public interest in freedom of expression also applies to other forms of confidential information, including government and commercial information**.

13. Surveillance Devices

Proposal 13-1

The ALRC proposes that surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.

The APF considers that the current State and Territory surveillance device and workplace surveillance laws are inadequate for protecting the privacy of Australians, and should be reformed as a matter of priority. The lack of uniformity in the laws between the States and Territories has created considerable uncertainty about what is legally permissible and what is impermissible surveillance. This has been compounded by an apparent reluctance to inform the public about the laws and the allocation of limited resources to enforce the laws. The lack of consistency in State and Territory laws poses difficulties both for victims of unjustified surveillance and for those lawfully able to use surveillance devices. **While it is important to remove inconsistencies and promote uniformity, this must not be at the expense of reducing the level of protection of Australians against unjustified surveillance**. Given the proliferation of existing and emerging surveillance technologies and practices, it is more important than ever for Australians to have a high level of protection against surveillance unless there is a compelling public interest that justifies surveillance. In other words, uniformity should not be achieved at the expense of watering down Australians' rights to be free from unauthorised surveillance and any standardisation should be based on 'best practice' protection of privacy and not on 'lowest common denominator' protection.

The ALRC proposes that uniform offences should be introduced for the use of surveillance devices to monitor 'private activities'.

The APF agrees on the need for uniformity, provided that the weaknesses and inadequacies of the current laws are addressed.

In general, the APF considers that **what amounts to a 'private activity' should, in general, be determined by reference to whether there is a 'reasonable expectation of privacy' and not, for example, to whether an activity is carried on inside or outside a building** (which is the case with the current offence for optical surveillance in Victoria). Nevertheless, the APF acknowledges concerns with the 'reasonable expectation of privacy' benchmark. The main concern with adopting this standard is that it raises the possibility of privacy invasive technologies and practices which become entrenched changing what is regarded as 'reasonable', thereby shifting the playing field. While there may not be any one perfect solution to the problem of satisfactorily defining what amounts to a 'private activity', the APF urges the ALRC to give serious consideration as to how best to deal with the potential for privacy rights to be eroded by changing expectations, possibly instigated by business practices premised on large-scale privacy invasions.

As a final point, the APF submits that **offences for data surveillance should not be confined to law enforcement officers**, as is the case under the current Victorian and NT laws.

Proposal 13-2

The ALRC proposes that uniform surveillance device laws should adopt a technology-neutral definition of a 'surveillance device'.

The APF agrees that it is highly desirable to remove inconsistencies between State and Territory laws in the treatment of different kinds of surveillance devices and in the definitions of the types of devices. **The APF further considers that what amounts to a surveillance device should be determined by reference to the objective purpose of the device. The focus should be on whether or not the device is capable of surveillance** and not, for example, on distinctions

focused on the capability of technologies – whether hardware or software – for performing surveillance functions, and not on the specific features of particular technologies.

While flexible, technology-neutral definitions may be thought desirable at the general level, the APF has reservations about this, as there may well be particular technologies which give rise to specific concerns. Where this is the case, or where it is necessary to avoid doubt about whether or not a type of device is subject to the law, **there may be an inescapable need for definitions to refer to particular technologies**. In order to avoid the possibility of surveillance devices escaping regulation as a result of abstract legislative definitions, it may be advisable to include indicative lists of current and emerging technologies that are intended to fall within surveillance device laws.

The APF considers that **the proposed uniform laws should apply to all existing and emerging technologies that are capable of monitoring and recording the activities of people and their data**. For example, the laws should make it clear that they apply to unjustified surveillance by means of drones, wearable devices, data surveillance devices or RFID devices. Where there are gaps in the law, such as the monitoring of communications over wireless local networks, these unintentional exceptions should be removed. Moreover, as multi-functional mobile devices proliferate, it is important that protections against widespread surveillance to be maintained, even if this means that devices formerly thought not to be surveillance devices are caught by the regulatory net.

Proposal 13-3

The ALRC proposes that uniform surveillance device laws should include a general offence proscribing surveillance or recording of private conversations or activities without consent.

The APF agrees with this proposal, provided that what is 'private' and what amounts to 'consent' are adequately defined. As indicated above, the APF considers that, in the absence of a more satisfactory test, 'private' conversations and activities should be defined by reference to whether there is a 'reasonable expectation of privacy'. In relation to 'consent', it is important that any consent be freely given and unambiguous, and not unnecessarily implied or inferred from surrounding circumstances. In this respect, the APF considers that an overly-lax approach to consent in Australian information privacy law has tended to normalise privacy-invasive practices as, in practice, individuals are often given little option but to agree to data processing.

The ALRC also proposes removing inconsistencies between State and Territory laws by removing exceptions that, in some jurisdictions, allow for the use of surveillance devices by parties to conversations or activities, which is known as 'participant monitoring'. **The APF endorses the removal of the anomalous participant monitoring exception**. As the ALRC points out, this results in unacceptable inconsistencies between the States and Territories**. The APF considers that, unless surveillance is subject to specific exceptions, it should not be covert and should only be conducted with the consent of all parties to a conversation or activity**. That said, the APF acknowledges that there may be limited circumstances in which there is a public interest in allowing participant monitoring, such as where it is reasonably necessary for the protection of the lawful interests of the principal party to a conversation or activity. The APF submits, however, that such exceptions should be carefully circumscribed so as to avoid the possibility of the exceptions swallowing the rule.

Proposal 13-4

The ALRC proposes that surveillance device laws should include a defence of responsible journalism, for surveillance in limited circumstances by journalists investigating matters of public concern and importance, such as corruption. This proposed defence appears to have been influenced by the *Reynolds* defence to actions for defamation under English law.

The APF supports the public interest activities of responsible journalists in investigating and reporting on matters of public interest, such as uncovering corruption. The APF does not support a broad or vague exception for journalists, however, on the basis that regular recourse to surveillance technologies may well lead to a 'slippery slope', which has been highlighted by unlawful and unacceptable activities of news organisations in the UK, as detailed in the *Leveson Inquiry*. The real concerns arising from the recent history of widespread unauthorised surveillance by media organisations in the UK suggest that **quite different considerations apply in determining the scope of defences to surveillance device laws than apply to defences to actions for defamation**.

The APF supports the creation of a public interest exception for the activities of journalists, but subject to the vital condition that it is satisfactorily confined, so that it does not act as an open invitation for media organisations to undertake surveillance of private activities and practices. We draw attention to the specific formulation in the APF's Policy Statement on Privacy and the Media of March 2009. The relevant segment of that Statement is attached to this document.

In particular, care would need to be exercised in defining who was entitled to an exception, as well as precisely limiting the circumstances in which surveillance might be permissible. While a level of surveillance for the purposes of uncovering corruption may be acceptable, there is obviously considerable room for debate about what might amount to corruption in this context. Given the potential for 'scope creep', there may be a case for limiting the exception to circumstances involving 'serious corruption'. In any event**, there is no case for surveillance where the activities are merely of interest to the public or likely to titillate the public interest**.

In addition, there are serious questions about the level of information or suspicion about corrupt behavior that might be needed in order for surveillance to be justified, especially given the potential for existing and emerging technologies to allow for widespread surveillance as part of 'fishing expeditions'. For example, it would seem that something more than mere speculation about the possibility of corruption should be required before the exception could be relied upon. It may be that any exception for the media should incorporate a 'reasonable suspicion' test – although, even then, difficult questions arise about the level of evidence required to substantiate a reasonable suspicion of corruption. Finally, the exception for responsible journalism should not be used as a Trojan horse for the reporting of private facts uncovered as part of a corruption investigation. For example, surveillance of a public figure may well reveal personal information, such as information about an affair, which is unrelated to the allegations of corruption. The journalism exception should not be extended to allow for the publication of unrelated private information where there is no clear public interest in the information being published.

Question 13-1

The ALRC has asked whether the States and Territories should enact uniform surveillance laws, or whether the Commonwealth should legislate to cover the field?

The APF considers that the significant differences between the surveillance devices laws in the States and Territories, and the lack of attention given to law reform at the State and Territory level, **indicates that requiring agreement among the States and Territories is likely to lead to a protracted law reform process**. Given the importance of harmonising and updating surveillance devices laws**, the APF considers that the Commonwealth should take the lead in pursuing law reform in this area**. In the absence of a clear indication from the States and Territories to pursue law reform, the Commonwealth may need to legislate to cover the field**. The APF agrees with the ALRC (para [13.12) that uniform Commonwealth laws may be supported by the external affairs power, and supplemented by the communications power (s 51(v))**.

Proposal 13-5

The ALRC proposes that surveillance device laws should provide for courts to make orders for compensation or other remedial relief to victims of unlawful surveillance.

The APF agrees that surveillance device laws should incorporate a mechanism for awarding compensation, or other forms of relief, to victims of unauthorised surveillance. The APF considers that further attention needs to be given to the precise mechanism for providing victims with an effective means for seeking remedial relief. Given the history of inadequate enforcement of surveillance device laws, **the APF supports the introduction of a civil penalties regime for breaches of surveillance devices laws**. The introduction of a civil penalties regime would establish an effective mechanism for ensuring compliance with surveillance device laws. If the ALRC's proposal for introducing a statutory tort that applies to intrusion is accepted, victims of unauthorised surveillance could seek redress under this cause of action. Accordingly, **if a statutory tort is not introduced, there is an even stronger case for establishing a civil penalties regime under uniform surveillance device laws**. Even if a statutory tort were to be introduced, the APF considers that there are advantages in establishing an additional affordable mechanism for victims of unauthorised surveillance to seek appropriate relief.

Question 13-2

The ALRC has asked whether local councils should be empowered to regulate the installation and use of surveillance devices by private individuals?

The APF considers that surveillance devices, including CCTV cameras installed for security purposes, should be regulated by strong uniform national laws. Accordingly, the APF considers that any regulation at the local council level must comply with standards established under uniform surveillance device laws. While there may be scope for local councils to be involved with resolving disputes about the installation and use of some devices, this must not be at the expense of strong national standards.

The APF draws attention to its Policy Statement on Visual Surveillance, including CCTV, revised in January 2010, which declares the Principles necessary to provide effective control over these activities. The Statement is at http://www.privacy.org.au/Papers/PS-CCTV.html.

15. New Regulatory Mechanisms

Proposal 15-1

The ALRC proposes that the ACMA should be empowered, where there has been a privacy complaint under a broadcasting code of practice, to make a declaration that the complainant is entitled to compensation. **The APF supports the proposed new power for the ACMA to award compensation, and notes that the APF's previous submission that that the cause of action for a 'serious invasion of privacy' should also be an 'interference with privacy' under the *Privacy Act 1988* (Cth) would have the result that the Privacy Commissioner/AIC would have such a power.**

The APF notes that, as a result of the exemption for journalism in s 7B(4) of the *Privacy Act 1988* (Cth), the ACMA is the primary agency responsible for the regulation of invasions of privacy by media organisations. The APF further notes that in its 2008 report on privacy, the ALRC recommended that the *Privacy Act* be amended to provide that media privacy standards must deal *adequately* with privacy in the context of the activities of a media organization, and that this recommendation has not been acted upon.

Given the journalism exemption in s 7B(4), the APF considers that it is essential for the regulatory powers of the ACMA to be brought into line with those of the OAIC. As the ALRC points out, this reform is necessary to ensure that a person whose privacy is invaded in breach of a broadcasting code of practice is entitled to compensation. The APF considers that this reform will only be effective, however, if the journalism exemption in the *Privacy Act* is amended to ensure that broadcasting codes adequately protect privacy.

The ALRC has proposed that the ACMA should only be empowered to make a declaration where there has been a serious invasion of privacy. As the ACMA would only be empowered to make a declaration in the event of a breach of a broadcasting code of practice, the APF disagrees with the proposed limitation to serious invasions of privacy. **In our view, a complainant whose privacy has been invaded in breach of a broadcasting code of practice should be entitled to compensation without needing to establish that the invasion is 'serious'.**

Proposal 15-2

The ALRC proposes that a new APP be inserted into the *Privacy Act* to require an APP entity to provide a simple mechanism for an individual to request the destruction or de-identification of personal information that was provided to an APP entity by the individual. The ALRC also proposes that an APP entity that receives such a request should be required to take reasonable steps to destroy or de-identify the relevant personal information in a reasonable time. As the ALRC explains, the proposed new principle would supplement existing APPs 13 (correction) and 11.2 (deletion or de-identification). **The APF supports the new proposed new APP.**

The APF agrees that the new principle is necessary to ensure that an APP entity adequately responds to requests to delete or de-identify personal information beyond the circumstances dealt with in APPs 13 and 11.2. The new principle is likely to be especially important in the context of personal information that an individual has posted to a social networking site. In such circumstances it is important for a regulatory mechanism to be established to ensure that social networking service providers respond promptly and adequately to requests to delete or de-identify information. In this respect, the APF notes that it is commonly much too complex for people to satisfactorily delete

content from their own social media accounts.[15] Given the well-reported difficulties people commonly encounter in deleting information, the APF considers that the obligation imposed on APP entities should be to respond to a request in an *adequate* time rather than a reasonable time. Moreover, in order to ensure that users are able to take advantage of mechanisms for deleting personal information, the APF considers that APP entities, and especially social network service providers, should be required to provide prominent and accurate information about how the mechanism works, including in the entity's privacy policy. To avoid doubt, and to ensure that the proposed new APP is effective, it may be necessary to amend the *Privacy Act* to make it clear that the APPs apply to social networking service providers that hold the personal information of Australians, regardless of where that information is stored or processed.

Question 15-1

The ALRC has asked whether the proposed new APP requiring deletion or de-identification should also require an APP entity to take steps with regard to third parties with which it has shared the personal information. **In relation to this question, the APF submits that, when destruction or de-identification of the information does occur, an APP entity should be required to inform the individual that he or she is entitled to require the APP entity to inform any third parties to which it has provided the information that the information has been destroyed or de-identified, with a request from the APP entity that the third party do likewise, and to inform them that they have done so. The APP entity should be required to inform the individual of the answers from third parties that it receives.**

APP6 sets out the circumstances in which an APP entity may use or disclose personal information, including circumstances in which disclosure is permitted without the consent of the individual concerned. The APF further considers that where an APP entity has disclosed information to third parties in breach of the APPs, and received a request to delete the information, then the entity should be required to take reasonable steps to ensure that the information is also deleted by third parties to whom the information has been disclosed, and to inform the individual concerned of the steps taken. The APF notes that such an obligation would be consistent with the obligation imposed on controllers under Article 17 of the proposed *General Data Protection Regulation,* which is currently being considered for adoption in the European Union.

The APF considers that merely because disclosure of personal information by an APP entity to third parties is permitted by the APPS, including APP6, does not mean that the entity has no further responsibility for the information. This is because an individual may not be aware of all relevant facts and circumstances at the time the personal information was collected. Consequently, where an individual requests the deletion of personal information from the APP entity that collected it, the APF considers that the entity should be required to take reasonable steps to provide the individual with a list of third parties who have received the information, and to notify third parties to which it has disclosed the information that a request to delete the information has been received.

Question 15-2

The ALRC has asked whether a regulator should be empowered to order the removal of material from a website or online service where an individual has requested the removal and the request has not been complied with. **In relation to this question, the APF submits that a regulator should be so empowered. Consistent with the APF's previous submission that that the cause of action for a 'serious invasion of privacy' should also be an 'interference with**

[15] See, for example, Jennifer Golbeck, 'I Decided to Delete All My Facebook Activity: It Was Hard', *Slate,* 1 January 2014.

privacy' under the *Privacy Act 1988*, the APF submits that the Privacy Commissioner/AIC should be a regulator so empowered, subject to the right of appeal to the AAT. This is not a radical proposal in the Asia-Pacific: South Korea's data privacy law already has at least as strong a provision.

The ALRC has suggested that a take-down order may be justified where:

- the regulator receives a complaint from an individual;
- the individual has attempted, without success, to have the material removed by the organisation which controls the website or online service; and
- the regulator considers that the posting of the information constitutes a serious invasion of privacy, having regard to freedom of expression and other public interests.

The APF notes that the cyber-safety consultation paper released by the Commonwealth in January 2014[16] raised the possibility of a notice and take-down regime designed to ensure rapid removal of material that is harmful to a child from social media sites.

The APF agrees that privacy concerns regarding social networking sites are sufficiently serious to justify considering the implementation of a notice and take-down regulatory regime, which may result in removal of material where a social networking service operator fails to respond adequately to a complaint. The APF also agrees with the ALRC that caution should be exercised in establishing any such regime so as to avoid unduly inhibiting freedom of expression. In particular, a legislative regime such as that proposed by the ALRC may create incentives for service operators to respond to all requests by simply removing material, even where there are important countervailing interests, including interests in freedom of expression. It may be that, as with the regime suggested in the cyber-safety consultation paper, any such regime should be confined to large social media sites. As such entities are well-resourced, and have commercial interests in individuals posting personal information, they might be expected to resist adopting policies involving the large-scale automatic removal of material. Another safeguard that could be contemplated would be to implement a counter-notification regime, whereby third parties with an interest in material not being removed could object to a request for removal.

A notice and take-down regime, in and of itself, is unlikely to adequately address the serious privacy invasions that have arisen online. Any such regime must be accompanied by other measures which contribute to the protection of privacy online. For example, the APF considers that large social media sites should be required to implement effective complaints mechanisms, with adequate enforcement by a regulator in the event of non-compliance. In this respect, the APF does not consider that the *Cooperative Arrangement for Complaints Handling on Social Networking Sites* (the Protocol), which has been in place since early 2013, provides adequate or appropriate protection for users of social networking services.

If a notice and take-down regulatory regime were to be introduced for serious invasions of privacy, the APF considers that it should be consistent with any other such existing or contemplated regimes. Consequently, if a regime were to be introduced to deal with cyber-bullying, it would be appropriate for responsibility for the privacy regime to be given the same regulator. In addition, the APF considers that it is essential to ensure that the regulator responsible for such a regime be equipped with adequate resources and powers of enforcement.

Related to this proposal, the APF reiterates its submission in response to Question 27 in the ALRC's Issues Paper, that 'the definition of "personal information" in the *Privacy Act 1988* (Cth) should be amended so as to confirm that the information will remain personal information, despite any steps to anonymise it, if there is any significant possibility that it

may be re-identified in future.'[17] Such a change is necessary if the proposed new APP is to be fully effective, and remain so in light of technological changes in re-identification methods.

Proposal 15-3

The ALRC proposes that the *Privacy Act 1988* (Cth) be amended to confer additional functions on the AIC to, where the Commissioner considers it appropriate, to assist the court as amicus curiae and to intervene in court proceedings.

The APF supports these two proposals but considers that they are too limited because they do not address the problem of litigants of limited means, and the deterrent against bringing an action where awards of costs against the plaintiff are possible. The APF's proposals that the Privacy Commissioner have jurisdiction to investigate and rule on complaints of 'serious invasions of privacy' would address this problem. If this proposal is not adopted, so that court actions are the only option then the ALRC proposal needs to be strengthened by inclusion of changes such as are found in the 2012 amendments to Hong Kong's *Personal Data (Privacy) Ordinance*, allowing the Commissioner to grant appropriate applications to act on behalf of a plaintiff (or fund representation by counsel) in a compensation claim before a court. The costs of the Commissioner or counsel in such matters are a first charge on any compensation awarded.

Other regulatory reforms

Small business

The ALRC notes that the recommendation in the 2008 ALRC report, *For Your Information,* for removing the small business exemption from the *Privacy Act 1988* (Cth) has yet to be acted on. The ALRC suggests that, given developments in digital communications and the digital economy since the 2008 report, the small business exemption should be given further consideration.

The APF submits that the exemption for small business significantly compromises Australia's information privacy regime. As the ALRC pointed out in its 2008 report, removal of the small business exemption would bring Australian law into line with the law in other comparable jurisdictions, including New Zealand, the European Union and Canada. Furthermore, there is no compelling evidence, from jurisdictions where there is no small business exemption, to suggest that compliance costs are a significant burden. Accordingly, the APF submits that the ALRC's 2008 recommendation for removing this unjustified exemption should be implemented as a matter of priority.

[17] APF supported this as follows: 'This change would have a profound effect, on an 'industrial' scale, as a response to the challenges to privacy posed by so-called 'big data' and the techniques of data analytics/data mining. These techniques are the foundations of the personalisation of interactions, sometimes known as 'mass personalisation', and the identification and re-identification of individuals in the Internet/mobile communications environments. In addition, practices such as the increasing potential for metadata to be matched with other data to identify an individual's online behaviour currently fall largely outside the regulatory

An extended complaints process for the OAIC

In its submission to the Issues Paper, the AIC/Privacy Commissioner supported a new 'complaints model' under which an intrusion into seclusion would constitute an 'interference with the privacy of an individual' under the *Privacy Act 1988* (Cth). As the ALRC acknowledges [15.52], this proposal has considerable advantages, not least of which is providing a cost-effective means for addressing serious invasions of privacy.

As explained in our detailed response to Proposal 9-1 (above), the APF strongly supports the proposal that the AIC/Privacy Commissioner be given jurisdiction over *all* serious invasions of privacy, as an important alternative means for resolving complaints relating to the proposed tort. The APF further submits that this proposal can be expeditiously implemented by providing that the the cause of action for a 'serious invasion of privacy' is an 'interference with privacy' for the purposes of the *Privacy Act 1988* (Cth).

Additional new regulatory measure: Individuation not just identification

The APF reiterates its submission to the ALRC in in response to Question 27 in the ALRC's Issues Paper concerning 'individuation not just identification' as the basis of 'personal information':

> 'The definition of 'personal information' in the *Privacy Act 1988* (Cth) should be amended so that it no longer is restricted to information which has the capacity to identify an individual, but also includes information which provides the capacity (whether by itself or in conjunction with other information) for another entity to interact with an individual on an individualised or 'personal' basis. If an entity can send a person emails, SMS messages or the like, or configure their experience of a website or other digital facility, on the basis of information that depends upon their individual experience, history, preferences or other individuating factors, then such information should be regarded as personal information, and the interaction with them should be regarded as the use of such personal information. Such individuated/personalised interactions are now the basis of all marketing conducted on the Internet and via mobile telecommunications, and as such constitute one of most significant serious invasions of privacy in the digital era. Moreover, the Foundation considers that rapidly emerging marketing practices, including online behavioural advertising, psychographic profiling and predictive analytics, mean that this issue requires urgent attention. A change, along the lines suggested here, which is under consideration in current European law reform processes, would involve a major strengthening of privacy protection relevant to this reference.'

The title of the ALRC's reference refers to 'the digital era' and this proposed change would make the Privacy Act more resistant to irrelevance through technological change than any other, and would be likely to cause a significant reduction in serious invasions of privacy in the digital environment by requiring business practices to come within the scope of the Privacy Act.

Extract from APF Policy Statement re Privacy and the Media
At http://www.privacy.org.au/Papers/PS-Media.html

Revision of 26 March 2009

The justification for the collection or publication of personal data must be based on one or more of the following:

Consent. The consent of the individual concerned is sufficient justification for personal data to be collected and published. Particularly for sensitive personal data, express consent is needed. For less sensitive data, implied consent may be sufficient. Where multiple individuals are directly identified (rather than merely indirectly implicated), the consent of each is needed.

Relevance to the Performance of a Public Office. This encompasses all arms of government, i.e. the parliament, the executive and public service, and the judiciary. The test of relevance is mediated by the significance of the role the person plays. Publication of the fact that a Minister's private life has been de-stabilised (e.g. by the death of a family member, marriage break-up, or a child with drug problems) is more likely to be justifiable than the same fact about a junior public servant. Publication of the identities and details of other individuals involved (e.g. the person who died, or the child with drug problems) is also subject to the relevance test, and is far less likely to be justifiable.

Relevance to the Performance of a Corporate or Civil Society Function of Significance. The relevance test needs to reflect the size and impact of the organisation and its actions, the person's role and significance, and the scope of publication.

Relevance to the Credibility of Public Statements. Collection and disclosure of personal data may be justified where it demonstrates inconsistency between a person's public statements and their personal behaviour, or demonstrates an undisclosed conflict of interest.

Relevance to Arguably Illegal, Immoral or Anti-Social Behaviour. This applies to private individuals as well as people performing functions in organisations. For example, in the case of a small business that fails to provide promised after-sales service, or a neighbour who persistently makes noise late at night, some personal data is likely to be relevant to the story, but collection and disclosure of other personal data will be very difficult to justify.

Relevance to Public Health and Safety. For example, disclosure of a person's identity may be justified if they are a traveller who recently entered Australia and they are reasonably believed to have been exposed to a serious contagious disease.

Relevance to an Event of Significance. For example, a 'human interest' story such as a report on bush fire-fighter heroics, may justify the publication of some level of personal data in order to convey the full picture. Generally, consent is necessary; but where this is impractical and the story warrants publication, the varying sensitivities of individuals must be given sufficient consideration. This is especially important in the case of people caught up in an emergency or tragedy, who are likely to be particularly vulnerable.

Any Other Justification. A justification can be based on further factors. However, in the handling of a complaint, any such justification must be argued, and the onus lies on the publisher to demonstrate that the benefits of collection or publication outweigh the privacy interest.

Mitigating Factors. The outcome of the above relevance tests may be affected by the following factors:

Self-Published Information. Where an individual has published personal data about themselves, that person's claim to privacy is significantly reduced. However it is not extinguished. In particular

and the less widely the individual reasonably believed the information to have been made available. Further, only information published by the individual themselves affects the relevance test, not publication by another individual, even a relative or close friend or associate.

Public Behaviour. Where data about an individual arises from public behaviour by that individual, the person's claim to privacy is reduced. However, public behaviour does not arise merely because the individual is 'in a public place'. For example, 'public behaviour' does not include a quiet aside to a companion in a public place.

Attention-Seekers. In the case of people who are willingly in the public eye (e.g. celebrities and notorieties), consent to collect and publish some kinds of personal data may be reasonably inferred. But this does not constitute 'open slather', and active denial of consent must be respected. This mitigating factor is not applicable to the attention-seeker's family and companions.

CAVEAT. Special care is needed in relation to categories of people who are reasonably regarded as being vulnerable, especially children and the mentally disabled, but depending on the circumstances, other groups such as homeless people and the recently bereaved.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/