Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

14 February 2014

Prof. John Williams
Director
SA Law Reform Institute
Adelaide Law School
University of Adelaide
Adelaide SA 5005

SALRI@adelaide.edu.au

Dear Prof. Williams

Re: A statutory cause of action for invasion of privacy

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

The APF has been active for some years on the question addressed by your current Reference. APF's Policy Statement on the matter was published in July 2011. It provided a Submission to the Department of Prime Minister & Cabinet in November 2011, and a further Submission to the ALRC in relation to its current Reference, in November 2013. We note that your Issues Paper of December 2013 makes a brief reference to the APF's November 2011 Submission.

The APF is an entirely voluntary organisation, and because of the very large number of issues on which its views are sought, it has to carefully ration the time of its Board and Committee members.

The APF regrets that it is currently only able to provide brief responses to a few of the more crtitical Questions raised in your Issues Paper on pp. 75-79. However, the APF's prior documents on the matter form part of this Submission, and are attached.

Should there be specific aspects on which the APF's views would be particularly significant, we would be pleased to provide a more detailed response.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 6916 Chair@privacy.org.au

Australian Privacy Foundation

A statutory cause of action for invasion of privacy

Brief Responses to Some Key Questions

14 February 2014

The APF's Responses below need to be read on conjunction with the following attachments:

- Policy Statement of July 2011
- Submission to the Department of Prime Minister & Cabinet (PM&C) of November 2011
- Submission to the ALRC of November 2013

1. Should there be a law giving people a right of action against an individual or organisation who invades their personal privacy?

Yes.

The APF's Policy Statement addresses this question.

Further detail is in the Submission to the PM&C, at 2.4 on pp. 2-5.

2. What do you mean by personal privacy in this context?

The APF follows Morison (1973) in referring to privacy as the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. This approach valuably avoids the distractions that are inevitable when the word 'right' is included. Privacy protection is always an exercise in balance among multilple interests of multiple parties.

US approaches such as those of Posner in particular, but also Solove, have proven to be of little practical value, and map poorly to Australian needs. Privacy has multiple dimensions. An approach that the APF finds much more practical is to distinguish:

- privacy of the physical person
- privacy of personal communications
- privacy of personal data
- privacy of personal behaviour
- privacy of personal experience

The word 'privacy' is frequently mis-used to refer to 'data privacy' alone.

Some jurisdictions have data privacy laws in place, which provide weak 'data protection' (and, in the case of the Commonwealth, they will be even weaker with effect from mid-March 2014).

South Australia has no law in place, but merely an inadequate Cabinet Administrative Instruction, and an ineffectual Committee whose primary function is to authorise exceptions. Only Western Australia provides less data protection than South Australia.

All jurisdictions have some limited protections for the privacy of personal communications, but they are primarily incidental provisions within statutes that authorise breaches of communications privacy.

Some jurisdictions provide limited protections for behavioural privacy in the form of surveillance devices statutes. South Australia provides the least behavioural privacy protection of any jurisdiction, in that it has only an ancient Listening Devices Act.

4. Are there any particular examples of kinds of invasions of personal privacy that you consider should fall within a cause of action for invasion of privacy?

See the PM&C Submission at 2.4(2) and (3) on pp. 3-5.

5. How serious should the invasion of personal privacy be for a right of action to arise?

APF's position is that "the threshold of 'highly offensive' is too high".
See the PM&C Submission at 2.5 on p. 5, and at 3(4) on p. 7

7. Should the Act define the concept of personal privacy?

Privacy is a notion of very wide scope, as discussed in our response to Q. 2 above.
Its interpretation is dependent on context, and decisions are best made in each particular context.
APF's position is that time spent on definitions is largely wasted.
APF supports the position adopted in almost all statutes of avoiding a definition of the term.

8. Should there be a list in the Act of what amounts to an invasion of personal privacy?
9. If so, should it be a complete list or simply give examples?
10. If there is a list, should it at least include: ...

APF's position is that "An expressly non-exhaustive list of activities should be included in the legislation, so as to clearly illustrate the breadth of the cause of action".
The breadth of the privacy notion is such that under no circumstances should an exhaustive or exclusive list be embodied in the law.
The expressly non-exclusive list should include <u>at least</u> the items in Q. 10.
See the PM&C Submission at 3(9a) and the examples in 3(9b), both on p. 8.

11. Should it be possible for a negligent breach of personal privacy to be actionable? Or should only intentional or reckless breaches be actionable?

APF's position was stated in the PM&C Submission at 3(7) on p. 8:
"It is essential that both intentional and reckless breaches be subject to the cause of action.
"We further submit that an action should not fail merely because a breach was negligent. A serious lack of care that falls short of recklessness should be actionable (subject to the other requirements), but the remedies should reflect the extent of the carelessness".

See also the Submission to the ALRC, at Q.9 on p. 7.

12. Should only natural persons be able to take action for invasion of personal privacy?

APF's position was stated in the PM&C Submission at 3(16) on p. 9:
"It is essential that the cause of action be restricted to natural persons.
"Privacy is a fundamental human right, recognised in the UDHR, ICCPR, and many other human rights instruments. Under no circumstances must the concept of privacy rights be debased by permitting the right to be applied in any manner whatsoever to legal persons".

See also the Submission to the ALRC, at Q.18 on pp. 9-10.

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/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/

Version of 21 July 2011

Background

The need for effective privacy protections has been well-understood for 40 years - since Sir Zelman Cowen's 'The Private Man' in 1969.

The courts have failed to develop a tort of privacy, and parliaments have provided only very limited and very weak legislation. Privacy Commissioners have not been provided with powers to solve problems, and in any case recent federal Privacy Commissioners do not have a strong record of working to protect people's privacy.

All three Law Reform Commissions have recognised that the time has come to enable people to take legal action against unreasonable behaviour by companies, governments and other individuals. (ALRC 2008, NSWLRC 2009, VLRC 2010). They have framed the new right so as to avoid the risk of a chilling effect on media freedom, by including a 'public interest defence' and a relatively high threshold of 'serious intrusion' that is offensive to a reasonable person. See, in particular, the ALRC's Recommendation No. 74.

Despite the LRCs' careful work, the media have mounted opposition campaigns against the proposal. There have been statements by proprietors and executives, and hysterical articles in the press – in some cases by otherwise steady and reponsible reporters and commentators. As has been well-documented, politicians have long lived in fear of the media, particularly the Murdoch press. The proposal has accordingly sat on the back burner for a considerable time.

The revelations about serious misbehaviour by UK News Corporation reporters, and quite possibly by managers and executives, has revived interest in the right to action. On 21 July 2011, the Australian Government announced that it will release a Discussion Paper on the matter (Media Release, mirrored here).

The APF's Position

Privacy protection in Australia is seriously inadequate. On the other hand, the privacy interest must always be carefully balanced against other important interests. In particular, privacy protections must not obstruct the legitimate role of the media in holding to account governments, corporations and individuals in positions of power.

The APF strongly supports the introduction of a right of action that has the following characteristics:

- it must available to individuals, but not to legal persons such as companies
- it must enable a court to grant injunctions, award damages, and impose ~~penalties~~ exemplary or punitive damages [clarified 24 Oct 2013]
- it must require the court to balance the privacy interests of the litigant against other important interests, including and especially 'the public interest'
- it must provide a clear framework and criteria for evaluating a defence that an invasion of privacy is justified in the public interest

The APF published its Policy Statement on 'Privacy and the Media' in March 2009. This includes what it believes to be an appropriate interpretation of the public interest. It will be submitting this to the Government for consideration.

In addition, the APF strongly supports the removal of the media exemption from the existing provisions of the Privacy Act, as per the ALRC's carefully drafted Recommendation No. 42.

Discussion Points

1. The privacy right of action is not specifically about the media; but it must apply to the media as well as every other individual and organisation

2. Media commentators originally reacted hysterically against the proposal, and have grossly misrepresented what it is, and

what impact it would have

3. Media freedoms are crucial to a free society, and crucial to privacy interests. Privacy advocates are intent on ensuring that reasonable behaviour by journalists and publishers is supported, and is not prevented or constrained by the new right

4. The APF remains open to discussions with the media and other interested organisations about its Policy Statement on 'Privacy and the Media', with a view to the development of a common position on how the public interest should be defined

---

Created: 21 July 2011 - Last Amended: 21 July 2011 by Roger Clarke - Site Last Verified: 11 January 2009

Site Map - This document is at http://www.privacy.org.au/Directory/Page.html - Privacy Policy

Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

4 November 2011

Mr Richard Glenn
Head, Privacy and FOI Policy Branch
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Dear Richard

Re: A Statutory Cause of Action

I refer to the Issues Paper made available in September.

I attach the APF's Submission.

Our Submission is open.

We applaud the Department's policy on confidentiality as far as it goes, but urge that the Department adopt a refinement to it.

Where a submission is made in confidence, we submit that the Department should decline to accept and consider it, unless all of the material that it contains is sufficiently sensitive to justify suppression from public view.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

A Statutory Cause of Action

Submission of 4 November 2011

Executive Summary

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

The APF strongly supports the creation of a statutory cause of action, and made public statements to that effect in 2007 and 2011. Important reasons supporting a statutory cause of action are:

- there are many offensive intrusions for which no privacy protective mechanism exists
- many dimension of privacy lie outside the narrow scope of existing privacy laws. These include the privacy of the physical person, the privacy of personal behaviour, and the privacy of personal communications
- many organisations, many categories of actions, and individuals generally, are exempt from existing privacy protective mechanisms
- most existing privacy protections are ineffectual, due to weak legislation, lack of resources, lack of enforcement powers, and timidity on the part of privacy oversight agencies
- such non-privacy actions as exist (e.g. defamation, confidence, negligence) fail to fill the void

Many offensive intrusions arise in society generally, including leaks of personal data, surveillance of behaviour, interference with a person's body, and abuse of powers by government agencies.

In addition, there are many instances of offensive intrusions by the media. These are of great concern where they affect 'ordinary people', although the scope of the cause of action must also extend to 'celebrities'. Further, contrary to the assertions frequently made by media commentators, concerns about media abuses originate much more frequently in relation to 'tabloid media' and 'infotainment', and much less often in relation to 'quality outlets' and genuine 'news-reporting'.

The need for the cause of action must be seen as arising primarily in relation to society as a whole. The media must be understood to be just one specific area of application, and one which to which a clear, strong and extensive definition of the public interest defence applies, as articulated in the APF's Policy Statement on 'Privacy and the Media' of July 2009.

Clear Recommendations were made by ALRC, over 3 years ago. We submit that, in order to achieve the most desirable form of the cause of action, the legislation should reflect the following refinements to the ALRC's Recommendations:

- the threshold of 'highly offensive' is too high, as it would exclude many offensive intrusions that are deserving of remedies. A plaintiff should be required to show that:
  - (a) the plaintiff has in relation to conduct or information a reasonable expectation of privacy; and
  - (b) the act complained of is sufficiently serious to cause, to a person of ordinary sensibilities, substantial offence or distress, in the relevant contex ('offensive intrusion');
- the balancing of interests should be left to the defences. To integrate it into the cause of action would place an unfair burden of proof on the plaintiff – often to prove a negative. However, see our answer to question 8 below concerning factors to be taken into account;
- intention and recklessness, but also a serious lack of care, should all be actionable
- there should be no exemptions for any categories of organisations or actions
- the cause of action must be limited to individuals, because privacy is a human right

There is a pressing need for the statutory cause of action. The APF urges the Government to table legislation as soon as practicable, in order to implement the protections at an early date.

Australian Privacy Foundation

A Statutory Cause of Action

Submission of 4 November 2011

1. Introduction

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

The APF strongly supports the creation of a statutory cause of action.

This was made clear as long ago in 2007, in the APF's submission to the ALRC, at http://www.privacy.org.au/Papers/ALRC-DP72-0712.pdf.

Further, in July 2011, the APF published a Policy Statement, at: http://www.privacy.org.au/Papers/PRoA.html:

> Privacy protection in Australia is seriously inadequate. On the other hand, the privacy interest must always be carefully balanced against other important interests. In particular, privacy protections must not obstruct the legitimate role of the media in holding to account governments, corporations and individuals in positions of power.
>
> The APF strongly supports the introduction of a right of action that has the following characteristics:
> - it must available to individuals, but not to legal persons such as companies
> - it must enable a court to grant injunctions, award damages, and impose penalties
> - it must require the court to balance the privacy interests of the litigant against other important interests, including and especially 'the public interest'
> - it must provide a clear framework and criteria for evaluating a defence that an invasion of privacy is justified in the public interest

The APF strongly welcomes effective consultation processes. On the other hand, we believe that there has been more than enough discussion. We urge the Government to table legislation as soon as practicable, in order to maintain momentum and implement these protections at an early date.

Clear Recommendations were made by ALRC over 3 years ago.

We submit that, in order to achieve the most desirable form of the Cause of Action, the legislation should make several refinements to the ALRC's Recommendations. Details of the refinements that we propose are presented below.

2. Responses to the Issues Paper

This Submission adopts the following approach:

- it discusses key points in each of the Issue Paper's sections in turn
- it provides answers to the specific questions asked
- it is supplemented by copies of:
  - the APF's Policy Statement re a Privacy Right of Action, of July 2011
  - the APF's Policy Statement re Privacy and the Media, of March 2009

2.1 Introduction (pp. 7-8)

The APF welcomes the recognition that a statutory cause of action is a missing element in the Australian legal framework for privacy protection, and has been identified as such by three Law Reform Commissions.

In the area of information privacy, the enactment will fill a gap.

However, it will also establish a foundation for the protection of dimensions of privacy for which no coherent framework is currently in place. This is further addressed in sub-section (4) immediately below, and in our answer to Question 9b.

We appreciate the government's desire to reinforce the case for the cause of action and to review the variations in the models proposed by the three Commissions, in order to refine the design of the scheme.

However, we urge the government to move quickly and directly to implementation.

2.2 The Current Privacy Context (pp. 9-12)

We believe that this section of the paper provides a reasonable summary of the context.

However, we strongly disagree with the statement on page 12 that "In many cases, recordings of private information or collections of data are also handled in ways consistent with an entity's privacy policy, with the Commonwealth Privacy Act, or with equivalent laws".

This is an area of major inadequacy in the current privacy regime. In some (and we would argue many) cases, personal infomation is <u>not</u> handled in accordance with law and organisations' own policies. Non-compliance is commonplace, due partly to the weak and inadequately resourced monitoring and enforcement regimes under existing laws.

Organisations in both the public and private sectors know that the sanctions for privacy breaches are minor to the point of being non-existent, and in any case the chances of detection are low.

Hence organisations, quite rationally, adopt a risk management approach and give a low priority to privacy compliance and training. As we argue below, the introduction of a cause of action, and the experience of cases brought under the right, will help to focus management attention on privacy issues and will in time lead to higher levels of compliance.

2.3 The Present State of the Law ... (pp. 13-22)

We believe that this section provides a reasonable summary of the present state of privacy law.

We note that the overseas comparisons mostly support the introduction of a privacy cause of action.

2.4 Is There a Need ... (pp. 23-31)

There is a pressing need for a statutory cause of action.

The cause of action has been the subject of media reports in successive waves since 2005, corresponding with the ALRC Discussion Paper and later Report, the NSWLRC Discussion Paper and later Report, the VLRC Discussion Paper and later Report, and the Senate Committee on Online Privacy Hearings and later Report.

There has been a regrettable and unjustified focus in media reporting on the application of the cause of action to the media itself.

It is very important that consideration of the need for the cause of action focus primarily on society as a whole, with the media as just one specific area of application – albeit one in which the public interest defence will be particularly relevant.

We present in this sub-section information relating to:

- the reasons why the need arises
- examples of privacy abuses that arise in society generally
- examples of media behaviour that must be subject to the cause of action

(1) Reasons Why the Need Arises

The need derives from many factors, important among them the folllowing:

- many actions taken by organisations and individuals are highly privacy-invasive, and unjustifiably so, but either no mechanism exists at all for preventing them or enabling action against people who perform them, or alternatively a mechanism exists but is ineffectual
- some actions that are seriously and unjustifiably privacy-invasive lie outside the narrow scope of existing privacy laws. Important examples include:
  - invasions of the privacy of the physical person
  - invasions of the privacy of personal behaviour
  - invasions of the privacy of personal communications
  - invasions of privacy by organisations that are, or whose actions are, exempt from privacy law, such as law enforcement and national security agencies, most organisations in relation to their employees, and most small business in relation to their customers
  - invasions of privacy by individuals
  - invasions of privacy that are excluded from the scope of privacy oversight agencies by virtue of the very large numbers of jurisdictional limitations within privacy laws
- some actions that are seriously and unjustifiably privacy-invasive are nominally within-scope of a privacy oversight agency, but such protections as exist are ineffectual. Reasons for this include:
  - lack of resources in the hands of the privacy oversight agency
  - timidity on the part of the privacy oversight agency
  - lack of enforcement powers in the hands of the privacy oversight agency
- such non-privacy actions as exist (such as defamation, confidence and negligence) fail to fill the void, because they are variously inapplicable, fit very poorly to the need, or do not provide appropriate and effective controls and remedies

(2) Non-Media Examples

A privacy cause of action must be available in relation to any kind of action, harming any kind of privacy, performed by any natural or legal person. Only in that way can the cause of action create the opportunity for balance, and act as a brake on excessive behaviour.

There are many circumstances that the APF believes could give rise to application of the cause of action. Some important categories include:

- leaks of personal data from government agencies and private-sector organisations:
  - in circumstances in which the organisation has clearly failed its obligations in relation to the security of sensitive data
  - as a result of abuse of privilege by individual employees
- surveillance of an individual's actions (whether or not any personal data arises from the activity), including observation by individuals

- interference with a person's body, such as unjustified acquisition of samples of body fluids, e.g. for drug testing, or of biometric measures, e.g. for clocking on and off work
- abuse of powers by law enforcement and national security agencies, such as unjustified arrest, unjustified humiliation, unjustified search and identification procedures and unjustified deprivation of liberty. Some recent or well-known examples in this particular category, who must be able to pursue cases under such a cause of action (whether or not they have recourse under any other cause of action), include the following:
    - Prashant Cherkupalli, reported on at: http://www.smh.com.au/national/student-illegally-detained-20111023-1menm.html
    - Muhamed Haneef
    - Musa Konneh, reported on at: http://www.smh.com.au/technology/technology-news/class-action-filed-over-glitch-wrongly-jailing-young-people-20110608-1fs1h.html
    - Cornelia Rau
    - Vivian Solon

There is accordingly a pressing need for a statutory cause of action that applies generally to all organisations, and all individuals, without exception. It is of course vital that many other conditions and threshold tests be applied, but these are the subject of other parts of the the Issues Paper and of this Submission.

(3) Media Excesses

There are all-too-frequent instances of seriously and unjustifiably privacy-invasive actions by the media. However, contrary to the assertions frequently made by media commentators, these arise only infrequently in 'quality outlets' and genuine 'news-reporting', and when they do they are in most cases follow-on reporting about 'stories' that have been first published elsewhere.

The vast majority of seriously and unjustifiably privacy-invasive actions by the media originate outside 'quality outlets' and genuine 'news-reporting', in the grey zones of 'info-tainment' and outright 'creative entertainment', which have represented a very large proportion of the output of media organisations in recent years.

Here are some **individuals who have a 'media profile'** and who have been the subject of serious media excesses:

- Lara Bingle
- Belinda Emmett
- Andrew Ettinghausen
- Candice Falzon
- Deltra Goodrem
- Pauline Hansen
- Nicole Kidman
- Jess Origliasso
- Nick Riewoldt
- Sonny Bill Williams

While most of the examples that come to public attention relate to 'celebrities', there are also many that involve 'ordinary' people but which, for that reason, are less memorable and less readily re-discovered when preparing a Submission of this nature.

It is essential that the debate about a cause of action not be unduly influenced by questions as to whether the 'victim' has a public profile. That may (or may not) be relevant to a public interest defence, but it is not relevant to whether or not there has been an offensive intrusion.

Here are a couple of recent examples of **individuals who are not otherwise well-known**, but who have been the subject of serious media excesses:

- the 14-year-old girl interviewed by Jackie O and Kyle Sandilands
- Madaleine Pulver
- the 14-year-old boy charged with drug possession in Bali: http://www.theaustralian.com.au/news/nation/give-bali-accused-some-space-lawyer/story-e6frg6nf-1226181938888

We draw to attention one glaring instance that **originated in what is arguably a 'quality outlet'**, which unsuccessfully sought to justify publication on the basis of it being 'news-reporting' on a matter with an overriding public interest:

- David Campbell

In all of these cases, the disclosures, and in many cases also the collection methods, appear from the coverage to have been seriously and unjustifiably privacy-invasive actions. Moreover, we believe that public opinion largely agrees with that contention.

Whether actions by any of these individuals under a privacy cause of action would have succeeded cannot of course be certain – that would be for the courts to determine. Circumstances and considerations would come to light during proceedings that are not typically reported – hence the importance of a proper judicial process, rather than 'trial by media'.

The Australian Press Council and ACMA have comprehensively demonstrated their inadequacies, ACMA particularly so in the case of David Campbell. Even career-hardened journalists were aghast that Channel 7 escaped scot-free.

The APF sought a dialogue with the media industry and profession in early 2009, with a view to the establishment of much stronger bases for gauging the public interest. The APF's Policy Statement is at http://www.privacy.org.au/Papers/Media-0903.html, and attached to this Submission. It proved impossible to even achieve meaningful responses from either the media industry or the media profession, let alone dialogue.

As a general statement, self-regulation is an excuse, not a solution. The media have proven themselves to be incapable of conducting the process well enough to enable it to be projected even as a half-decent excuse.

There is accordingly a pressing need for the statutory cause of action to apply generally, including to the media, without exception. It is of course vital that many other conditions and threshold tests be applied, but these are the subject of other parts of the the Issues Paper and of this Submission.

2.5 Elements of the Cause of Action (pp. 24-38)

We address several aspects of this section in our answers to Questions 4-7, below.

The definition of the privacy action should be in general terms, but the threshold of 'highly offensive' is too high, as it would exclude many intrusions that a reasonable person would regard as objectionable and deserving of remedies.

A plaintiff should be required to show that in all the circumstances:

(a) the plaintiff has in relation to conduct or information a reasonable expectation of privacy; and

(b) the act complained of is sufficiently serious to cause, to a person of ordinary sensibilities, substantial offence or distress, in the relevant context.

The assessment of how a 'person of ordinary sensibilities' would react must be context specific. For example, a person who just experienced an accident or the loss of a loved one may be particularly sensitive.

2.6 ... Relevant Factors (pp. 39-40)

We address several aspects of this section in our answer to Question 8 below.

2.7 ... the Types of Invasion ... (p. 41)

It is essential that the cause of action be broad enough to cover all dimensions of privacy. It must not be restricted, for instance, to the publication of private facts – which is the type of privacy breach that has most commonly been at issue in the cases that have come before the courts to date.

We address several aspects of this section in our answers to Question 9 below.

2.8 Defences and Exemptions (pp. 42-44)

We address several aspects of this section in our answers to Questions 10-11 below.

2.9 Remedies (pp. 45-46)

We address several aspects of this section in our answers to Questions 12-14 below.

2.10 Resolving Matters Without Resort to Litigation (p. 47)

We address several aspects of this section in our answer to Question 15 below.

2.11 Other Issues (pp. 48-50)

We address several aspects of this section in our answers to Questions 16-19 below.

Class Actions

Provision should be made for representative or class actions, with appropriate rules, to address the many privacy intrusions that affect multiple individuals. A different cap on damages should apply.

3. Responses to Specific Questions

The text of our Submission above should be read in conjunction with the answers provided below. In some cases, it has been appropriate to repeat some segments of text in both places.

(1) Do recent developments in technology mean that additional ways of protecting individuals' privacy should be considered in Australia?

Yes.

Developments such as social media and cloud computing, and the increasing use of biometrics, CCTV and mobile devices, while they may offer benefits, have also increased pressure on privacy, and existing privacy laws are not adequate to provide the level of protection that Australians expect.

This is, however, not the only reason why the statutory cause is essential. Others include:

- the inceasingly privacy-invasive behaviour of organisations, whether or not the behaviour is motivated or enabled by the availability of new technologies
- the clear gaps that already exist in the privacy protection offered by existing information privacy and other laws
- the failure of a common law tort to emerge, despite four decades of public concern and earnest analysis in law journals

(2) Is there a need for a cause of action for serious invasion of privacy in Australia?

Emphatically Yes.

This is comprehensively addressed in section (4) above.

(3) Should any cause of action for serious invasion of privacy be created by statute or be left to development at common law?

The idea that a common law tort might emerge has been discussed in the literature for 40 years. But almost nothing has happened. And in any case, the courts can only deal with cases that come before them, and hence any common law tort that emerged would deal in a piecemeal and unsatisfactory manner with the problems, and would adapt very slowly to future changes in context.

It is also highly likely that individual courts would be unable to achieve balance between privacy and other interests, and that the outcomes would be not only highly uncertain but also in some instances inappropriate from a public policy perspective.

It is essential that the cause of action be created by statute, in order to carefully sculpt the cause of action to the public policy need.

(4) Is 'highly offensive' an appropriate standard for a cause of action relating to serious invasions of privacy?

No.

Highly offensive is too high a threshold, and would exclude many intrusions that a reasonable person would regard as objectionable and deserving of remedies.

A plaintiff should be required to show that, in all the circumstances:

(a) the plaintiff has in relation to conduct or information a reasonable expectation of privacy; and

(b) the act complained of is sufficiently serious to cause, to a person of ordinary sensibilities, substantial offence or distress, in the relevant context.

(5) Should the balancing of interests in any proposed cause of action be integrated into the cause of action (ALRC or NSWLRC) or constitute a separate defence (VLRC)?

The balancing of interests should be left to the defences. Integrating this balancing into the cause of action would unfairly place a burden of proof on the plaintiff – often to prove a negative. However, see our answer to question 8 below concerning factors to be taken into account.

(6) How best could a statutory cause of action recognise the public interest in freedom of expression?

Freedom of expression, and other important public interests, can be adequately protected by well crafted statutory defences. See our answer to question 10 below.

(7) Is the inclusion of 'intentional' or 'reckless' as fault elements for any proposed cause of action appropriate, or should it contain different requirements as to fault?

It is essential that both intentional and reckless breaches be subject to the cause of action.

We further submit that an action should not fail merely because a breach was negligent. A serious lack of care that falls short of recklessness should be actionable (subject to the other requirements), but the remedies should reflect the extent of the carelessness.

(8) Should any legislation allow for the consideration of other relevant matters, and, if so, is the list of matters proposed by the NSWLRC necessary and sufficient?

Of the list of relevant matters suggested by the NSWLRC, some would be appropriate factors to be specified as needing to be taken into account in establishing whether the primary test of 'offensive intrusion' has been met, but they should not be separate tests.

Other matters in the list, such as the claimant's public profile, are more appropriately left to the defence.

The legislation should not preclude the courts from interpreting the law in such a manner that additional matters that may be relevant can also be considered.

(9a) Should a non-exhaustive list of activities which could constitute an invasion of privacy be included in the legislation creating a statutory cause of action, or in other explanatory material?

An expressly non-exhaustive list of activities should be included in the legislation, so as to clearly illustrate the breadth of the cause of action. Such a legislative approach has proven successful, in various contexts, both in Australia and overseas.

(9b) If a list were to be included, should any changes be made to the list proposed by the ALRC?

A non-exhaustive list of activities should include at least the following (all of which deliberately refer to a person's private life, which must remain the focus of the cause of action):

(a) there has been an intrusion into an individual's home, family or otherwise private life;

(b) an individual has been subjected to surveillance in their home, family or otherwise private life;

(c) an individual's private written, oral or electronic communication has been interfered with, misused or disclosed;

(d) sensitive facts relating to an individual's private life have been disclosed.

(10) What should be included as defences to any proposed cause of action?

A non-exhaustive list of defences should be included in the legislation. The list should include versions of all the defences recommended by the three Law Reform Commissions, appropriately reconciled and integrated.

In addition, clearer and fuller expressions of the defences for freedom of speech in the public interest, and freedom of artistic expression are needed. Attention is drawn to the formulations in the APF's Policy Statement of 26 March 2009, copy attached.

(11a) Should particular organisations or types of organisations be excluded from the ambit of any proposed cause of action ... ?

No.

There should be no total or even partial exemptions for any organisations or activities.

(11b) Should ... defences be used to restrict its application?

Yes.

The defences will be sufficient to protect other public and private interests.

(12) Are the remedies recommended by the ALRC necessary and sufficient for, and appropriate to, the proposed cause of action?

All the remedies suggested by the ALRC should be available.

(13) Should the legislation prescribe a maximum award of damages for non- economic loss, and if so, what should that limit be?

There should be cap on the amount of damages for non-economic loss. This would help to dispel the alarmism being spread by media organisations that a privacy cause of action would be a 'honeypot', giving rise to actions motivated more by avarice than by genuine harm, as defamation law appears to have been before the introduction of caps.

(14) Should any proposed cause of action require proof of damage? If so, how should damage be defined for the purposes of the cause of action?

There should be no requirement for proof of damage, as some privacy intrusions will simply be inherently offensive, irrespective of any particular harm.

(15) Should any proposed cause of action also allow for an offer of amends process?

Yes.

An offer of amends process would be an appropriate inclusion which should result in acknowledgement of inappropriate behaviour, and the settlement of many actions without the private and public costs of full court proceedings.

(16) Should any proposed cause of action be restricted to natural persons?

Yes.

It is essential that the cause of action be restricted to natural persons.

Privacy is a fundamental human right, recognised in the UDHR, ICCPR, and many other human rights instruments. Under no circumstances must the concept of privacy rights be debased by permitting the right to be applied in any manner whatsoever to legal persons.

(17) Should any proposed cause of action be restricted to living persons?

We are inclined to support the analysis of the NSWLRC, to the effect that there should be no right of action on behalf of deceased persons.

However, it is important that this limitation not be framed in such a way as to compromise actions in relation to offensive intrusions into the privacy of other individuals. Of particular concern is the privacy of next-of-kin and close friends of a deceased person.

(18) Within what period, and from what date, should an action for serious invasion of privacy be required to be commenced?

Generally, we support the recommendation of the VLRC for a three year limitation period, from the date of the relevant conduct, to be the normal rule.

However, we submit that actions should be able to be commenced outside that period, if the plaintiff only became aware of the conduct more than three years after it occurred. In such cases, a limitation period of one year after becoming aware may be appropriate.

(19) Which forums should have jurisdiction to hear and determine claims made for serious invasion of privacy?

There should be the maximum possible choice of jurisdiction, including but not limited to the Federal Magistrates court, in order to minimise costs and procedural barriers in appropriate cases.

APF Policy Statement re a Privacy Right of Action
Version of 21 July 2011

Background

The need for effective privacy protections has been well-understood for 40 years - since Sir Zelman Cowen's 'The Private Man' in 1969.

The courts have failed to develop a tort of privacy, and parliaments have provided only very limited and very weak legislation. Privacy Commissioners have not been provided with powers to solve problems, and in any case recent federal Privacy Commissioners do not have a strong record of working to protect people's privacy.

All three Law Reform Commissions have recognised that the time has come to enable people to take legal action against unreasonable behaviour by companies, governments and other individuals. (ALRC 2008, NSWLRC 2009, VLRC 2010). They have framed the new right so as to avoid the risk of a chilling effect on media freedom, by including a 'public interest defence' and a relatively high threshold of 'serious intrusion' that is offensive to a reasonable person. See, in particular, the ALRC's Recommendation No. 74.

Despite the LRCs' careful work, the media have mounted opposition campaigns against the proposal. There have been statements by proprietors and executives, and hysterical articles in the press – in some cases by otherwise steady and reponsible reporters and commentators. As has been well-documented, politicians have long lived in fear of the media, particularly the Murdoch press. The proposal has accordingly sat on the back burner for a considerable time.

The revelations about serious misbehaviour by UK News Corporation reporters, and quite possibly by managers and executives, has revived interest in the right to action. On 21 July 2011, the Australian Government announced that it will release a Discussion Paper on the matter (Media Release, mirrored here).

The APF's Position

Privacy protection in Australia is seriously inadequate. On the other hand, the privacy interest must always be carefully balanced against other important interests. In particular, privacy protections must not obstruct the legitimate role of the media in holding to account governments, corporations and individuals in positions of power.

The APF strongly supports the introduction of a right of action that has the following characteristics:

- it must available to individuals, but not to legal persons such as companies
- it must enable a court to grant injunctions, award damages, and impose penalties
- it must require the court to balance the privacy interests of the litigant against other important interests, including and especially 'the public interest'
- it must provide a clear framework and criteria for evaluating a defence that an invasion of privacy is justified in the public interest

The APF published its Policy Statement on 'Privacy and the Media' in March 2009. This includes what it believes to be an appropriate interpretation of the public interest. It will be submitting this to the Government for consideration.

In addition, the APF strongly supports the removal of the media exemption from the existing provisions of the Privacy Act, as per the ALRC's carefully drafted Recommendation No. 42.

Discussion Points

1. The privacy right of action is not specifically about the media; but it must apply to the media as well as every other individual and organisation
2. Media commentators originally reacted hysterically against the proposal, and have grossly misrepresented what it is, and what impact it would have
3. Media freedoms are crucial to a free society, and crucial to privacy interests. Privacy advocates are intent on ensuring that reasonable behaviour by journalists and publishers is supported, and is not prevented or constrained by the new right
4. The APF remains open to discussions with the media and other interested organisations about its Policy Statement on 'Privacy and the Media', with a view to the development of a common position on how the public interest should be defined

APF Policy Statement re Privacy and the Media
Version of 26 March 2009

Preliminary Comments

Freedom of the press is a vital component of democracy.

There must be constraints, but they must be finely judged, in order to ensure that inappropriate behaviour in business and government can be exposed.

Privacy is a key human value, and one that is often not appreciated until it is lost. It is important that privacy be sufficiently protected.

Finding appropriate balances between openness and privacy is challenging, because of the enormous diversity of contexts, and the highly varying levels of concern different people have about different aspects of their privacy.

The Need

A framework is needed within which the media are able to work when making decisions about whether the collection of personal data, and the publication of personal data, unreasonably infringes privacy. That framework needs to be filled out with guidelines in relation to particular categories of people, data and contexts. The framework and guidelines need to be brief, clear and practical. They must not put the media in a straitjacket, but must enable them to exercise professional judgement in each situation as it arises.

The APF declares below the Framework it considers to be appropriate. The APF further proposes an indicative set of Guidelines to accompany and articulate the Framework.

These are presented in full knowledge of the existence since 2001 of the Australian Press Council (APC)'s Statement of Principles and Privacy Standards. The APF's position is that, after a decade's experience:

- detailed guidance is necessary
- the Framework and Guidelines need to apply to all media
- a comprehensive, gradated range of sanctions is necessary
- complaints schemes must be credibly independent of the organisations and individuals that are subject to the regulation, and complaint determinations must be appealable
- the APC does not provide adequate guidance, and any that may exist in the broadcasting field is seriously inadequate
- the existing self-regulatory and co-regulatory schemes (i.e. that operated by the APC, and the broadcasting codes administered by ACMA under s. 123 of the Broadcasting Services Act) have not satisfied these requirements

The Framework

The term *the media* is used in this document in a comprehensive manner, to refer to organisations and individuals publishing on a professional basis, through print, radio, television, web-sites and other media, and their employees and contractors.

Increasingly, organisations and individuals outside the media are performing much the same functions as the media, in a less formal manner. Appropriate balances need to be applied to the media right now, so that the standards can be applied to the general public in the near future.

The term *personal data* refers to data that can be associated with an identifiable human being. It is used in a comprehensive manner, in order to encompass all data forms such as text, audio, image and video.

1. The media must not seek, and must not publish, personal data unless a justification exists.
2. The justification:
    - must be based on 'the public interest', not on 'what the public is interested in'
    - must be sufficiently clear
    - must be of sufficient consequence that it outweighs the person's interest in privacy
    - must be of sufficient consequence that it outweighs any other conflicting interests such as public security and the effective functioning of judicial processes
    - must reflect the Guidelines applicable at the time

- must not claim reliance on a prior publication, but rather must stand on its own

3. In order to facilitate the handling of complaints, the media must be able to provide the justification for seeking, and for publishing, personal data, as described immediately above.
4. Internal complaints mechanisms must exist.
5. External complaints mechanisms must exist, which must be suitably resourced, must operate appropriate processes in a timely manner, and must be credibly independent from the complainee.
6. The consideration of a complaint about a specific instance of collection or publication of personal data must take into account information provided by the complainant, the justification presented, the context, the Guidelines applicable at the time the act in question occurred, and prior instances of comparable situations.
7. Appropriate forms of action must be available when complaints are upheld. The primary recourse needs to be published acknowledgement of inappropriate behaviour, and apology. In the case of privacy intrusions that are serious, blatant or repeated, a gradated series of sanctions is necessary, including professional rebuke, and the award of adequate (but not excessive) damages against corporations and against individuals.

Guidelines

The diversity of contexts is enormous. On the other hand, great depth of experience has been accumulated. It is not tenable for the pretence to be sustained that 'there are no rules'. It is acknowledged, however, that the 'rules' need to be expressed in qualified terms, that professional judgement needs to be applied, and that reasonable exercise of professional judgement needs to be taken into account as an important mitigating factor, even where a particular act is subsequently judged to have been inappropriate. The Guidelines focus on publication within Australia.

The following are provided as indicative Guidelines, in order to convey the sense of what the APF considers to be fair balances between the vital need for free media and the high value of personal privacy.

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, justification becomes more difficult the longer the elapsed time since the self-publication took place, 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.

Resources

ACMA (2009) 'Broadcasting Codes Index' Australian Communications and Media Authority, 2009, at http://www.acma.gov.au/WEB/STANDARD/1001/pc=IND_REG_CODES_BCAST

APC (2009) 'Statement of Principles', Australian Press Council, 2001-2009, at http://www.presscouncil.org.au/pcsite/complaints/sop.html

"For the purposes of these principles, 'public interest' is defined as involving a matter capable of affecting the people at large so they might be legitimately interested in, or concerned about, what is going on, or what may happen to them or to others"

APC (2009) 'Privacy Standards', Australian Press Council, 2001-2009, at http://www.presscouncil.org.au/pcsite/complaints/priv_stand.html

APF (2007a) 'Submission to the Australian Law Reform Commission's Review of Privacy – Answers to questions in ALRC Issues Paper 31' Australian Privacy Foundation, January 2007, at pp. 14-15 of http://www.privacy.org.au/Papers/ALRC_IP31_070202.pdf

APF (2007b) 'Submission to 'Australia's Right To Know' Coalition's Independent Audit into the State of Media Freedom in Australia' Australian Privacy Foundation, August 2007, at http://www.privacy.org.au/Papers/ARKC-MediaFreedom-0708.pdf

APF (2007c) 'Supplementary Submission to 'Australia's Right To Know' Coalition's Independent Audit into the State of Media Freedom in Australia' Australian Privacy Foundation, October 2007, at http://www.privacy.org.au/Papers/ARKC-MediaFreedom-0710.pdf

APF (2007d) 'Submission to the Australian Law Reform Commission re the Review of Australian Privacy Law – Discussion Paper 72' Australian Privacy Foundation, December 2007, at p. 68 of http://www.privacy.org.au/Papers/ALRC-DP72-0712.pdf

Ofcom (2005a) 'The Ofcom Broadcasting Code 2008 – Section 8: Privacy' [U.K.] Office of Communications, 2005, at http://www.ofcom.org.uk/tv/ifi/codes/bcode/privacy/

> "Meaning of 'warranted':" ... where broadcasters wish to justify an infringement of privacy as warranted, they should be able to demonstrate why in the particular circumstances of the case, it is warranted. If the reason is that it is in the public interest, then the broadcaster should be able to demonstrate that the public interest

outweighs the right to privacy. Examples of public interest would include revealing or detecting crime, protecting public health or safety, exposing misleading claims made by individuals or organisations or disclosing incompetence that affects the public"

"Meaning of 'legitimate expectation of privacy':Legitimate expectations of privacy will vary according to the place and nature of the information, activity or condition in question, the extent to which it is in the public domain (if at all) and whether the individual concerned is already in the public eye. There may be circumstances where people can reasonably expect privacy even in a public place. Some activities and conditions may be of such a private nature that filming or recording, even in a public place, could involve an infringement of privacy. People under investigation or in the public eye, and their immediate family and friends, retain the right to a private life, although private behaviour can raise issues of legitimate public interest."8.2 Information which discloses the location of a person's home or family should not be revealed without permission, unless it is warranted."8.3 When people are caught up in events which are covered by the news they still have a right to privacy in both the making and the broadcast of a programme, unless it is warranted to infringe it. This applies both to the time when these events are taking place and to any later programmes that revisit those events."8.4 Broadcasters should ensure that words, images or actions filmed or recorded in, or broadcast from, a public place, are not so private that prior consent is required before broadcast from the individual or organisation concerned, unless broadcasting without their consent is warranted".

"Suffering and distress"8.16 Broadcasters should not take or broadcast footage or audio of people caught up in emergencies, victims of accidents or those suffering a personal tragedy, even in a public place, where that results in an infringement of privacy, unless it is warranted or the people concerned have given consent."8.17 People in a state of distress should not be put under pressure to take part in a programme or provide interviews, unless it is warranted."8.18 Broadcasters should take care not to reveal the identity of a person who has died or of victims of accidents or violent crimes, unless and until it is clear that the next of kin have been informed of the event or unless it is warranted."

"People under sixteen and vulnerable people"8.20 Broadcasters should pay particular attention to the privacy of people under sixteen. They do not lose their rights to privacy because, for example, of the fame or notoriety of their parents or because of events in their schools. ...

"Meaning of 'vulnerable people':"This varies, but may include those with learning difficulties, those with mental health problems, the bereaved, people with brain damage or forms of dementia, people who have been traumatised or who are sick or terminally ill."

Ofcom (2005b) 'The Ofcom Broadcasting Code 2008 – Guidance Notes: Section 8: Privacy' [U.K.] Office of Communications, 2005, at http://www.ofcom.org.uk/tv/ifi/guidance/bguidance/guidance8.pdf

"Private lives, public places and legitimate expectation of privacy "Privacy is least likely to be infringed in a public place. Property that is privately owned, as are, for example, railway stations and shops, can be a public place if readily accessible to the public. However, there may be circumstances where people can reasonably expect a degree of privacy even in a public place. The degree will always be dependent on the circumstances. "Some activities and conditions may be of such a private nature that filming, even in a public place where there was normally no reasonable expectation of privacy, could involve an infringement of privacy. For example, a child in state of undress, someone with disfiguring medical condition or CCTV footage of suicide attempt."

"Practice to follow 8.17 People in a state of distress "Even if grieving people have been named or suggested for interview by the police or other authorities broadcasters and programme makers will need to make their own judgements as to whether an approach to such people to ask them to participate in a programme or provide interviews may infringe their privacy."

PCC (2007) 'Code of Practice' [U.K.] Press Complaints Commission, 1991-2007, at http://www.pcc.org.uk/cop/practice.html

"Private places are public or private property where there is a reasonable expectation of privacy" (since January 1998).

PCI (2007) 'Code of Practice for Newspapers and Periodicals' Press Council of Ireland, 2007, at http://www.pressombudsman.ie/v2/presscouncil/portal.php?content=_includes/codeofpractice.php

"Principle 5.4 Public persons are entitled to privacy. However, where a person holds public office, deals with public affairs, follows a public career, or has sought or obtained publicity for his activities, publication of relevant details of his private life and circumstances may be justifiable where the information revealed relates to the validity of the person's conduct, the credibility of his public statements, the value of his publicly expressed views or is otherwise in the public interest."

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 a Patron (Sir Zelman Cowen), 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/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/

Australian Privacy Foundation

w e bsite : www.privacy.org.au

SUBMISSION TO ALRC ISSUES PAPER: *SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA*

Professor Barbara McDonald
Australian Law Reform Commission
Sydney

Dear Professor McDonald

The Australian Privacy Foundation welcomes the Australian Law Reform Commission's consultation regarding privacy. This document responds to the Commission's call in October 2013 for public comment on its 'Serious Invasions of Privacy in the Digital Era' Issues Paper.

The following paragraphs provide a background and overview before addressing specific questions in the Issues Paper. The Foundation would be happy to address any point in more detail.

The Australian Privacy Foundation

The Foundation is Australia's leading civil society organisation concerned with privacy. Its board includes legal practitioners, academics and information technology specialists. It has been an active contributor to national and state/territory privacy policy development over many years. It has a particular interest in the interaction of new technologies and social activity with privacy, data protection and confidentiality.

The Foundation operates on an apolitical basis.

In contributing to policy development the Foundation emphasises principles (for example as productive of regulatory coherence and respect for all Australians). It seeks to situate law enforcement, commercial and other activity within a principles-based legal framework.

In doing so it recognises the importance of law enforcement and problems that arise where public administration is based on bureaucratic convenience rather than a respect for the human rights and responsibilities highlighted by the ALRC in the consultation paper. Recognition of privacy is wholly consistent with good government, economic growth, a vibrant media and personal flourishing.

Summary

The Foundation strongly endorses establishment in national legislation of a cause of action for serious invasion of an individual's privacy which, for convenience, this submission shall generally refer to as a statutory tort.[1]

That tort has been recommended by a succession of law reform commissions and other bodies. Recurrent recommendation demonstrates that there is a substantive and significant need for the tort and that after wide consultation those bodies consider that legislation is both desirable and viable. The tort has not been ruled out by the High Court and could be accommodated under the national constitution.

As noted by the law reform commissions the tort will not inhibit effective law enforcement or national security activity. It will not inhibit the implied freedom of political communication, a freedom that the High Court and Supreme Courts have indicated is not absolute. There is no reason to believe that the tort will burden the legal system with inappropriate litigation.

The tort will provide coherence across the Australian jurisdictions, where there is major inconsistency including, for example, in surveillance devices legislation. The tort will also offset regulatory incapacity, in particular the very restricted scope of the *Privacy Act 1988* (Cth) – concerned with information privacy – and under-resourcing of the Office of the Australian Information Commissioner (OAIC). It will fill a long-standing gap in the common law protection of the right to privacy, which is not adequately covered by existing causes of action.[2] The Foundation further considers that an important role of the tort is in signalling to all Australians that privacy should be respected as a matter of rights and obligations; that 'signalling' function is likely to be as significant as any deterrent associated with damages under the tort.

Fundamentally, the tort offers an effective remedy for problems that are evident in Australian law, that are of concern to many Australians, and that have been acknowledged by both courts and law reform bodies over a considerable period of time. Criticisms of the tort are exaggerated and typically reflect vested interests.

Principles

The Foundation endorses the following principles identified by the ALRC:

- recognition of privacy as important for individuals to live a dignified, fulfilling and autonomous life;
- substantive public interest in the protection of individual privacy and confidentiality;
- the balancing of privacy with other values and interests, including the promotion of open justice, freedom of speech, the protection of vulnerable persons and national security and safety;
- consistency with international standards and obligations in privacy law;
- flexibility, adaptability and certainty in application and interpretation;
- coherence and consistency in the law applying throughout Australian jurisdictions;

[1] The APF recognises the debate concerning whether or not the statutory cause of action is properly classified as a 'tort', but does not address this issue in this submission: see, for example, NSW Law Reform Commission, *Invasion of Privacy* (Report 120), April 2009, pp. 41-3.
[2] D. Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339.

- access to justice for those affected by serious invasions of privacy.

Those principles are reflected in the Foundation's responses to the questions posed by the ALRC in the 2013 Issues Paper, as follows.

Question 1: What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

> The Foundation endorses the above principles in aggregate and considers that they should be interpreted and applied on a holistic basis. Privileging one attribute – such as convenience in the enforcement of civil or criminal law – over principles results in law and practice that lacks legitimacy and coherence. In moving beyond the current consultation paper the ALRC should resist suggestions to 'stack' rights in a hierarchy and accordingly, for example, privilege the interests of commercial broadcasters, connectivity providers and social network services or law enforcement personnel.
>
> The current Australian privacy regime is, from the perspective of the individual subject of the information, often rendered ineffective by lack of any real capacity for individuals to enforce it, and by a model of vast and complex exceptions to its principles, scope and jurisdiction. In the Foundation's view, a private right of action in the form of a statutory tort is the long-needed essential counterpart of the existing regulatory framework, one which promises to enable flexible adaptation to emerging developments in the democratisation and distribution of personal data collection and use arising from the profound changes delivered by digitisation, networking and mass access to ever more rapidly evolving technologies
>
> That said, Australian jurisprudence over the past forty years has demonstrated that courts are capable of dealing with tensions in the interpretation of public and private interest, for example regarding defamation, national security and confidentiality. Consistent with the reports of the Victorian Law Reform Commission, New South Wales Law Reform Commission and the ALRC itself the Foundation encourages the Commission to question hyperbole by representatives of vested interests who claim that establishment of the tort would cripple law enforcement, damage the implied freedom of political communication, erode Australia's national competitiveness or serve as a refuge for the guilty.

Question 2: What specific types of activities should a statutory cause of action for serious invasion of privacy prevent or redress? The ALRC is particularly interested in examples of activities that the law may not already adequately prevent or redress.

> Private causes of action for the protection of privacy in common law jurisdictions draw upon the four privacy torts first identified by William Prosser, and subsequently codified in the US *Second Restatement of the Law of Torts*.[3] The four torts are:
> - unreasonable intrusion upon the seclusion of another;
> - appropriation of another person's name or likeness;
> - unreasonable publicity given to another person's private life; and
> - publicity that unreasonably places another person in a false light before the public.
>
> Of these, the first and third torts are most closely related to protection of the right to privacy, with the second and third torts extending to protect interests in addition to privacy, such as commercial interests in an image or reputation.

[3] William Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

The Foundation considers that the rights and interests falling within the Prosser taxonomy are not adequately protected under current Australian law. As pointed out in the 2009 NSW Law Reform Commission Report, there are clear gaps in the protection of privacy under existing private law causes of action, including:

- uncertainty concerning whether or not the equitable action for breach of confidence is available where private information has been not obtained in circumstances importing a duty of confidentiality;
- the limitations in the action for intentional infliction of emotional harm, which prevent it from applying to intrusions that do not cause recognisable psychiatric harm; and
- the lack of actionability of intrusions, such as those at issue in *Kaye v Robertson,*[4] where unauthorised photographs were taken of a television personality lying injured in a hospital bed.

Moreover, the emergence of new technologies and applications, including drones and wearable devices, such as Google Glass, highlight and exacerbate the existing gaps in the law. It is likely, for example, that 'passive' monitoring by drones or wearable devices fall outside the parameters of existing causes of action, but nevertheless pose privacy risks that should be addressed.

Question 3: What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?

Consistent with the preceding comments, the Foundation advises against specifying activities that should be privileged by the Act. That advice does not mean that appropriate and proportionate law enforcement action should breach the cause of action. (As noted above the Foundation urges the ALRC to look critically at claims that the tort will have deleterious effects, claims that were made when the *Privacy Act 1988* (Cth) and state/territory privacy statutes were introduced and have been shown to be unfounded.)

In considering what is 'unduly' restrictive the Foundation notes weaknesses within the *Privacy Act 1988* (Cth) and other legislation that feature substantial formal 'carve-outs' and that are further undermined by incapacity (lack of power, resources and will) on the part of regulators such as the Commonwealth Privacy Commissioner (as part of the OAIC). It is highly undesirable that the scope for action regarding serious invasions of privacy be seriously eroded through major exemptions or by limiting the ability to bring an action by a regulator, such as the OAIC.

Question 4: Should an Act that provides for a cause of action for serious invasion of privacy (the Act) include a list of examples of invasions of privacy that may fall within the cause of action? If so, what should the list include?

Inclusion of a list of examples may be useful in guiding courts and more broadly in addressing unfounded anxieties about the purpose of the legislation or its scope. Inclusion of examples in the statute rather than merely in extrinsic aids to interpretation such as the Explanatory Memorandum and 2nd Reading Speech is not remarkable or inconsistent with Australian drafting practice.

The Foundation considers that the list should be clearly identified as non-exclusive and

[4] [1991] FSR 62.

non-exhaustive, ie courts should be able to deal with serious invasions of privacy that fall outside the list. This should be made abundantly clear in the legislation itself, as well as in any extrinsic material, so as to prevent the courts from adopting an overly-restrictive interpretation of any illustrative list. This approach is consistent with the Foundation's endorsement of flexibility as one of the principles underlying the Act.

Question 5: What, if any, benefit would there be in enacting separate causes of action for: misuse of private information; and intrusion upon seclusion?

The three Australian law reform commissions that have recommended enacting a private cause of action have adopted different approaches to the design of the cause of action. While the ALRC and the NSWLRC supported a single cause of action, the VLRC favoured two causes of action, broadly corresponding to Prosser's intrusion and publication torts.

The main disadvantage of separate causes of action is that they may be under-inclusive. The introduction of two causes of action for intrusion and publication may, for instance, result in some identifiable privacy breaches not being covered by either tort. In particular, there might be occasions where personal information is accessed and used, without there being any actionable intrusion or publication. The Foundation supports a single cause of action, as an appropriately drafted cause of action will prevent privacy harms from 'falling through the cracks'.

While separate causes of action can promote certainty and flexibility by, for example, allowing for defences to be specifically tailored, the Foundation considers that it is possible to achieve this within a single cause of action.

Question 6: What should be the test for actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?

Consistent with the principles noted above the Foundation considers that actionability should depend mainly on the identification of circumstances where there is a reasonable expectation of privacy. This is an objective test that also provides flexibility, and which can be interpreted by the courts to reflect both principles and evolving social practice.

In any event, a 'serious' invasion should not be predicated on identifiable psychiatric harm or other specific harm to the individual whose privacy has been invaded as, in the first instance, actionability should be addressing the invasion rather than the harm. The severity of the harm is a matter that is appropriately taken into account in determining remedies.

Regarding the invasion itself, the Foundation considers that the threshold for actionability should be left largely to the courts. In this respect, the Foundation considers that a requirement for the invasion to be 'serious' should provide a sufficient safeguard against trivial complaints, without the need for a more detailed test. A threshold based on the 'seriousness' of the invasion or breach should be sufficient to avoid the tort being so wide as to allow for actions by persons who are merely offended or embarrassed.

Question 7: How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that: competing public interests must be considered when determining whether there has been a serious invasion of privacy; or public interest is a defence to the statutory cause of action?

The Foundation considers that this matter can be addressed through reference in the Act to a requirement that public interest be considered by courts in dealing with action for serious invasion of privacy. That consideration should be undertaken on a holistic basis, ie not in a way that necessarily prioritises law enforcement or the implied freedom of political communication or the commercial media over respect for the individual whose privacy has been invaded.

The Foundation notes that Australian courts have successfully grappled with competing claims of public interest, in particular regarding publication by media organisations such as John Fairfax and the Australian Broadcasting Corporation. Public interest should be a defence to the statutory cause of action but that interest must be recognised in terms of public good rather than in terms of public curiosity, media group ratings or bureaucratic convenience.

Upon analogy with the tort of defamation and the action for breach of confidence, the balance between the public interest in protecting the right to privacy and other rights and interests (including rights to freedom of expression) is best undertaken by including public interest as an affirmative defence, rather than as a balancing exercise undertaken within the parameters of the cause of action. One reason for this is that a defendant will usually be best placed to lead evidence relevant to whether or not a privacy breach is in the public interest. Moreover, adequate recognition of the right to privacy suggests that the onus of establishing that there is a public interest in a breach should lie with defendants.

Question 8: What guidance, if any, should the Act provide on the meaning of 'public interest'?

The Foundation considers that there are real dangers in attempting to compile a 'shopping list' of issues that may fall within a public interest defence. One of the dangers is that attempting to construct a list can open the door to special pleading by private interest groups. If it is considered that some illustrative examples may assist the courts in applying a public interest defence, this can always be addressed in extrinsic materials.

The main problem with a public interest defence is the potential for it to be interpreted in a way that undermines the right to privacy. This has clearly occurred in the United States where, due to the influence of the First Amendment, the 'newsworthiness' defence has effectively trumped the public disclosure tort. As the Foundation regards privacy as a fundamental right, the preferred approach is to require that all defences comply with the principle of proportionality. In the event that the proportionality principle is not adopted, some consideration could be given to limiting the defence to matters of 'legitimate public concern', as suggested by Gault P and Blanchard J in the New Zealand decision, *Hosking v Runting*.[5]

[5] [2005] 1 NZLR 1, 32.

Question 9: Should the cause of action be confined to intentional or reckless invasions of privacy, or should it also be available for negligent invasions of privacy?

The Foundation considers that the cause of action should encompass 'serious' invasions of privacy *per se* and should thus include negligent breaches. As noted above, concerns that the cause of action might encourage trivial or vexatious complaints can be dealt with by means of a threshold confining the action to 'serious' invasions or breaches.

Question 10: Should a statutory cause of action for serious invasion of privacy require proof of damage or be actionable *per se*?

The cause should be actionable *per se*. This approach best reflects the principles articulated by the ALRC. As a legal system we should be signalling that 'serious' invasion of privacy is abhorrent, irrespective of whether the subject of that invasion is highly resilient, is psychologically traumatised by the invasion or experiences financial injury.

Requiring proof of damage burdens potential litigants and is likely to deter some people from taking action over substantive invasions by well-funded parties. As explained in this submission, concerns that the cause of action may extend to everyday conduct that should not be actionable are best addressed by confining the action to 'serious' invasions or breaches.

Question 11: How should damage be defined for the purpose of a statutory cause of action for serious invasion of privacy? Should the definition of damage include emotional distress (not amounting to a recognised psychiatric illness)?

The action, and appropriate remedies, should be available where a person has suffered emotional distress, embarrassment or humiliation. Whenever there has been a 'serious' invasion of privacy, it should be possible for a complainant to obtain a remedy. The remedy must, of course, be proportional to the harm suffered.

Question 12: In any defence to a statutory cause of action that the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property, should there be a requirement that the act or conduct was proportionate, or necessary and reasonable?

Yes. Proportionality is an essential requirement, in relation to each and every defence.

The Foundation fully recognises and endorses the appropriateness of action by law enforcement and national security personnel, provided always that it is within an appropriate rights-based framework. The Foundation is, for example, on the public record as supporting instances where what would otherwise be regarded as invasive is legitimate and desirable in the public interest.

The Foundation cautions, however, about the danger of fundamentally weakening the tort through a 'carve-out' for particular interests. Given a majority in the relevant legislature it is a simple matter for a particular government to enact 'law and order' or 'national security' legislation that authorises representatives of the state to behave in

ways that raise legitimate and serious concerns regarding civil liberties. Those concerns can be best addressed through a requirement that the behaviour be proportionate, necessary and reasonable rather than based on what a particular agency or politician considers to be administratively convenient or electorally attractive.

Given an appropriate emphasis on rights-based principles, the Foundation considers that it is possible to identify a principled, context-specific balance on a case by case basis. In practice, the balance can be underpinned by a statutory requirement that, in order for the act or conduct to be justified it must be proportionate, necessary and reasonable.

Question 13: What, if any, defences similar to those to defamation should be available for a statutory cause of action for serious invasion of privacy?

As pointed out in the 2009 NSW Law Reform Commission report, defamation defences are not necessarily applicable to a privacy tort as privacy and defamation protect different interests.[6] For example, the defence of truth is clearly inapplicable to a privacy action. Moreover, some defamation defences – such as the defences of honest opinion and extended qualified privilege – would fall within a broad public interest defence.

The NSW Law Reform Commission proposed that that the following four 'defamation' defences should apply to a statutory cause of action for the protection of privacy:

- absolute privilege (for parliamentary and judicial proceedings);
- qualified privilege (for fair and accurate reports of proceedings of public concern);
- qualified privilege (duty/interest); and
- innocent dissemination.

As Butler explains, in a helpful table,[7] these defences are broadly analogous to defences to privacy torts under the US *Second Restatement*. While the first two of the above defences would likely be protected under a general public interest defence, the Foundation considers that specific defences may be justified as necessary to protect freedom of expression. The Foundation is, however, less convinced of the need to specifically include an analogue for the duty/interest form of qualified privilege, as this may best be dealt with under a public interest defence.

The Foundation considers that particularly difficult issues arise in relation to the liability of intermediaries, especially those involved in the dissemination of private material online. At this stage, the Foundation considers that the potential liability of intermediaries, including any form of accessorial liability, should be subject to further investigation, before any consideration is given to defences analogous to the defence of innocent dissemination. In this respect, the Foundation notes that the need for a defence of innocent dissemination arises as a result of strict liability for the publication of defamatory material. In circumstances where liability attaches to intermediaries, it may be appropriate to limit remedies where an intermediary complies with a prescribed procedure, such as a requirement to remove or 'take down' material.

[6] NSW Law Reform Commission, *Invasion of Privacy* (Report 120), April 2009, pp. 45.
[7] D. Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 385-6.

Question 14: What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?

The Foundation considers that, in general terms, an appropriately defined public interest defence is preferable to attempting to precisely define, in legislation, the circumstances in which privacy breaches may be justified. That assessment reflects the Foundation's emphasis on principle as noted above. The Foundation urges the ALRC to consider the tort on a holistic basis and to avoid a sectoral approach (ie by particular industry, medium or action) that risks rendering the tort incoherent or privileging particular interests over others.

Question 15: What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?

Provided the elements of the statutory cause of action, and defences, are appropriately defined, the Foundation does not see the need for exempting particular activities or types of activities.

Question 16: Should the Act provide for any or all of the following for a serious invasion of privacy: a maximum award of damages; a maximum award of damages for non-economic loss; exemplary damages; assessment of damages based on a calculation of a notional licence fee; an account of profits?

The Foundation considers that remedies should encompass damages (including exemplary damages), an account of profit, apology, retraction and injunction. The courts should be given sufficient flexibility to determine the most suitable remedies and, in this respect, the tort should be drafted in terms that do not unduly restrict the court's discretion.

Question 17: What, if any, specific provisions should the Act include as to matters a court must consider when determining whether to grant an injunction to protect an individual from a serious invasion of privacy? For example, should there be a provision requiring particular regard to be given to freedom of expression, as in s 12 of the *Human Rights Act 1998* (UK)?

Australian courts have not enshrined a broad, self-standing right to freedom of expression. This suggests that there may be some value in incorporating a provision such as s 12 of the *Human Rights Act 1998* (UK) in the statute, although the Foundation notes criticisms by figures such as Raymond Wacks in *Privacy & Media Freedom* (Oxford University Press, 2013). That said, considerations of 'prior restraint' must, in this context, appropriately take into account the extent to which privacy is uniquely vulnerable to any publication. Given this, it may be that freedom of expression is best addressed by means of the public interest defence.

Question 18: Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action? Who may bring a cause of action?

Apology and retraction should be included as non-monetary remedies, given that some subjects of serious invasion may not be interested in financial compensation. Apology has a valuable function in signalling acknowledgement of wrongdoing. So as to ensure proper redress, the remedies of apology and retraction should be complemented by a 'prominent publication' requirement.

Australian law provides for confidentiality in relation to corporations. Privacy as a human right should, however, be restricted to natural persons; there are alternate remedies for public/private organisations that may experience unauthorised access to and/or threatened/actual misuse of personal information. The action should not therefore be available to a corporate person in its own right.

Serious invasions should be actionable by a parent or guardian on behalf of those, especially minors, who lack legal capacity. The tort should also be actionable on a representative basis, given that multiple people may be the subject of a serious invasion by an organisation.

Question 19: Should a statutory cause of action for a serious invasion of privacy of a living person survive for the benefit of the estate? If so, should damages be limited to pecuniary losses suffered by the deceased person?

Given the Foundation's commitment to the protection of privacy as a fundamental right, the statutory tort should survive a deceased person, so as to allow for the appropriate vindication of that right post-mortem. As the introduction of a statutory tort will signal the unlawfulness of serious invasions, and as the courts can take the circumstances of a deceased person into account in awarding remedies, there is no need to limit remedies.

Question 20: Should the Privacy Commissioner, or some other independent body, be able to bring an action in respect of the serious invasion of privacy of an individual or individuals?

The Foundation is concerned that, given the costs of bringing an action before the courts, the introduction of a private cause of action, without more, may not adequately protect against serious invasions of privacy. Despite the Foundation's long-held concerns about regulatory failings in relation to the enforcement of complaints under the *Privacy Act 1988* (Cth), the Foundation supports giving the Commonwealth Privacy Commissioner the ability to bring 'own motion' actions before the courts for serious invasions of privacy. Over and above this, the Foundation considers that complainants should be given the option of pursuing a complaint for a serious invasion of privacy before the Privacy Commissioner. If a complainant is able to establish a breach of the statutory tort in proceedings before the Privacy Commissioner, this should amount to an 'interference of privacy', which would trigger the full enforcement regime under the *Privacy Act 1988* (Cth). Equipping the Privacy Commissioner with the power to address complaints of serious invasions of privacy will effectively supplement and reinforce the Commissioner's existing regulatory and enforcement functions. While complainants should have the option of bringing a complaint before the Privacy Commissioner, they should not thereby lose the right to bring an action before the courts. The proposed relationship between actions brought before the courts and complaints to the Privacy Commissioner is explained further in our response to Question 23.

Question 21: What limitation period should apply to a statutory cause of action for a serious invasion of privacy? When should the limitation period start?

Using the model of defamation action a one year period may be appropriate, with the limitation period starting from when the subject became aware of the invasion. Given increasing use of 'surveillance' technology that awareness may not arise until some time after the invasion has commenced or concluded.

Question 22: Should a statutory cause of action for serious invasion of privacy be located in Commonwealth legislation? If so, should it be located in the *Privacy Act 1988* (Cth) or in separate legislation?

For a coherent national regime it is essential that the cause of action be located in Commonwealth legislation. The Foundation considers that the Commonwealth has the constitutional power to introduce a uniform national regime.

If the Privacy Commissioner is to be given a regulatory role in receiving complaints for serious invasions of privacy, as is supported by the Foundation, the statutory tort should be introduced by appropriate amendments to the *Privacy Act 1988* (Cth). On the assumption that the existing enforcement regime under the *Privacy Act 1988* (Cth) should be available for serious invasions of privacy, incorporating the cause of action under the existing Act would simplify drafting. As explained elsewhere in this submission, it will also reinforce and extend the Privacy Commissioner's role as the regulatory agency responsible for dealing with privacy breaches.

Question 23: Which forums would be appropriate to hear a statutory cause of action for serious invasion of privacy?

The Foundation considers that private actions for breach of the statutory tort should be able to be brought before State and Territory Supreme Courts, the Federal Court of Australia and the Federal Circuit Court of Australia.

In addition, as explained elsewhere in this submission, the Foundation supports complainants being given the option of bringing a complaint relating to a breach of the statutory tort before the Privacy Commissioner. Such complaints should have the following features:

- If the Privacy Commissioner determines that there has been a breach of the statutory tort, this will constitute an 'interference with privacy', bringing all of the enforcement regime and remedies under the *Privacy Act 1988* (Cth) into play;
- At any time prior to a determination being made, the complainant should retain the option of bringing an action for a breach of the statutory tort before the courts;
- Both complainants and respondents should have a right to appeal from a determination of the Privacy Commissioner to the courts; and
- In such proceedings, findings of fact made by the Privacy Commissioner should be available to the court, consistent with the current provisions in the Act concerning enforcement of determinations, so that the matter does not need to be litigated *ab initio*.

Question 24: What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?

The Foundation recognises that some parties may wish to use alternative dispute resolution mechanisms, for example on the basis of cost, timeliness, stress or publicity. However, there should be no mandating of those mechanisms and in particular there should be no requirement for initial conciliation by the Privacy Commissioner. Of course, if both parties agree, they should have the option of conciliation under the *Privacy Act 1988* (Cth). As emphasised in this submission, the option of bringing a complaint under the procedures established under the *Privacy Act 1988* (Cth) should not prevent complainants from bringing an action before the courts.

Question 25: Should a person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation be permitted to bring or continue a claim based on the statutory cause of action?

The introduction of a private cause of action for the breach of privacy will provide private remedies where either none currently exist, or where existing legal protections are inadequate. The enforcement regimes under existing legislation - such as the Commonwealth, State and Territory information privacy laws – commonly have objectives additional to the vindication of a person's right to privacy. For example, Australia's information privacy laws are aimed, in part, at promoting good data management practices. Furthermore, the balances struck between the protection of the right to privacy and other rights and interests may differ, depending upon the particular legal regime. For example, the information privacy laws take into consideration the interests of government agencies and corporations in ways that may not be appropriate for a private cause of action. This suggests that a person who has received a ruling, or lodged a complaint, regarding a breach of privacy under existing laws should not be prevented from bringing a private action under a statutory cause of action. In this respect, it is important to bear in mind that the outcomes of complaints under existing statutory regimes can always be taken into account by the courts in the award of discretionary remedies.

No finding by the Privacy Commissioner in relation to any other interferences with privacy (including breaches of the APPs, credit reporting or TFN breaches, etc) should have any effect on the ability of a complainant to pursue a complaint or action concerning a serious interference of privacy pursuant to the statutory tort. The elements of the cause of action for the statutory tort are different from the elements of any other interference with privacy, so they must necessarily be decided independently of each other. However, where a court or the Privacy Commissioner has made findings of fact which are also relevant to a serious invasion of privacy, it should be possible for the court hearing that latter matter to take those findings of fact into account.

Question 26: If a stand-alone statutory cause of action for serious invasion of privacy is not enacted, should existing law be supplemented by legislation: providing for a cause of action for harassment; enabling courts to award compensation for mental or emotional distress in actions for breach of confidence; providing for a cause of action for intrusion into the personal activities or private affairs of an individual?

The Foundation considers that a statutory cause of action that is specifically designed to protect the right to privacy is preferable to both the current inadequate and piecemeal protection, and to the incremental development of other causes of action,

such as statutory recognition of an action for harassment or development of the equitable action for breach of confidence. While additional legislative recognition of the need to protect privacy would be welcome, the reference provides the ALRC with the opportunity to design a best practice, 'purpose specific' cause of action, rather than fiddling around the edges of existing actions.

Question 27: In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?

The title of the reference refers to 'the digital era' and, while there are many improvements that could be made to privacy protection in general, the following are suggested changes that are likely to have the most impact on serious invasions of privacy in the digital environment.

- ***Individuation not just identification.*** 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.

- ***Re-identification*** 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 (or used for the purpose of individuated/personalised interactions, as described in the above proposal). 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 net. A reform such as this would, accordingly, also involve a major strengthening of privacy protection relevant to this reference.

- ***Data breach notification.*** A hallmark of the past decade has been a massive increase in large-scale data breaches or disclosures by both public sector and private sector organizations, mainly due to the capacity that the Internet has provided for both the disclosure of information (both inadvertently and via 'hacking' and other malfeasance) and its subsequent widespread and rapid dissemination. Therefore, a major strengthening of privacy protection relevant to this reference would result from the enactment of provisions for the prevention and notification of data breaches, as in the Bill which was not able to be enacted by the completion of the previous Parliament, but which received unanimous support from the Parliamentary Committee that considered it. Some aspects of that Bill could no doubt be improved, as the Privacy Foundation submitted in relation to the Bill, but it was also worthy of support as a matter of principle.

- ***Surveillance.*** A major concern for the Foundation has been an increase in the sophistication, intrusiveness and pervasiveness of surveillance technologies and practices. While a range of Commonwealth, State and Territory laws apply to surveillance devices and practices, the most significant laws are the State and Territory surveillance devices and listening devices Acts.[8]

  The State and Territory regimes are inconsistent, outdated and poorly enforced. Some of the problems with the regimes were identified by the Victorian Law Reform Commission in its 2010 report on *Surveillance in Public Places,* which concluded, in relation to the Victorian Act, that:[9]

  "At present the SDA [*Surveillance Devices Act 1999* (Vic)] regulates the use of surveillance devices inconsistently—certain activities are prohibited while others are effectively permitted because the Act says nothing about them. Furthermore, breaches of the Act attract serious criminal sanctions, which have proven not particularly effective in regulating public place surveillance".

The Foundation considers that the terms of reference provide an opportunity for the ALRC to review, and make recommendations for enhancing and improving, the inconsistent and inadequate State and Territory regimes that regulate surveillance technologies and practices. Given the present and emerging threats to privacy and individual liberties posed by surveillance devices and practices it is unacceptable for regulation to continue to be based on a patchwork of weak, technologically-outdated, poorly-known and poorly-enforced laws. In reviewing the State and Territory regimes, the Foundation considers that the ALRC should take into account:

- the desirability of introducing a uniform, Australia-wide regime, and the legal avenues available to the Commonwealth for promoting consistency among the State and Territories;
- the need to strengthen the State and Territory regimes so that, for example, they uniformly prohibit participant monitoring and appropriately restricting the extent to which 'implied consent' can be used to excuse unjustified surveillance, including covert surveillance;

[8] *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Listening and Surveillance Devices Act 1972* (SA); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).
[9] Victorian Law Reform Commission, *Surveillance in Public Places,* Final Report (May 2010), [6.109].

- the desirability of introducing civil penalties, which may go some way towards redressing the inadequate enforcement of the criminal offences established under the current regimes;
- the need for the legislation to be updated so as to effectively regulate new and emerging surveillance technologies; and
- in the absence of an effective regulator, the possibility of individuals bringing private actions to enforce breaches of surveillance devices laws.

The Foundation notes that submissions by individual members are likely to address further additional ways in which the current laws and regulatory frameworks are lacking and can be strengthened to better protect against serious invasions of privacy.

Question 28: In what other innovative ways may the law prevent serious invasions of privacy in the digital era?

The terms of reference require the ALRC to have regard to: "Innovative ways in which law may reduce serious invasions of privacy in the digital era". The Foundation considers that this provides the Commission with an opportunity to consider measures to address some of the most serious existing and emerging threats to the right to privacy, including threats that pose significant challenges to existing legal paradigms.

Protecting against serious invasions of privacy in a society that is increasingly characterised by the use of pervasive privacy-invasive and surveillance technologies, especially in the online context, cannot depend solely on law and regulation. There is a demonstrable need for holistic and concerted policies that promote education and privacy enhancing technologies, and incorporate appropriate assessment of privacy invasive technologies. All too often, government and regulatory responses to threats to privacy rights have been half-hearted, piecemeal and inconsistent.

Nevertheless, despite the limitations of legal solutions, laws can play a vital role in both inhibiting privacy invasions and in public education. An area of particular concern is the ready availability of affordable technologies that enable private individuals to collect, process and disseminate personal information on an industrial scale. This is particularly evident with the widespread use of social media, although it is not confined to those applications. The extent to which private individuals may increasingly engage in large-scale processing of personal information calls out for innovative legal and social strategies.

A first step in addressing these issues may be to focus on the right of individuals to delete personal information about them, such as photographs and videos, which has been posted online, especially to social media sites. This has become popularly known as the 'right to be forgotten'. As part of a fundamental review of the European Union data protection framework, the European Commission has adopted proposals for a new General Data Protection Regulation, which includes a version of a right to be forgotten.[10]

In its 2008 report on Australian privacy law, the ALRC rejected the view that the *Privacy Act 1988* (Cth) should be extended to apply to individuals acting in a non-

[10] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (Brussels, 25 January 2012) 2012/0011(COD), art. 17.

commercial capacity.[11] At that time, the Commission also rejected the possibility of establishing a take-down notice regime that would apply to online personal information.[12] Acknowledging that a statutory cause of action would not adequately address the problems arising from the use and disclosure of personal information on the Internet, the ALRC confined itself to emphasising the importance of public education, especially in relation to the 'privacy aspects of using social networking sites'.[13]

The Foundation notes that, since the ALRC's report, the use of social networking has become more pervasive and, accordingly, the privacy threats posed by social media have become more apparent. Moreover, it is only since 2008 that proposals for introducing a legal 'right to be forgotten' have received serious policy consideration, with proposed legislation now being under active consideration in the European Union. The problems are therefore much better understood, as are the undoubted complexities of attempting to draft laws that apply to social media.

In the light of these developments, the Foundation considers that the ALRC should revisit the conclusions reached in the 2008 report. In doing so, the Foundation believes that the current reference provides an opportunity for the ALRC to consider:

- the extent to which a 'right to be forgotten' should be incorporated under Australian law;
- the appropriate means for incorporating such a right, including the possibility of its incorporation in the *Privacy Act 1988* (Cth);
- if such a right were to be introduced, the appropriate scope of the right, including how rights to freedom of expression online can be best safeguarded; and
- the appropriate role of intermediaries, including social networking operators and search engine operators, in protecting online privacy.

In relation to serious invasions of privacy online, the Foundation considers that it is absolutely essential for the ALRC to give due consideration to the need for intermediaries, especially social networking service providers, but also search engine providers, to take appropriate responsibility for commercial services and activities which are premised on privacy invasions. This means that not only should the potential liability of intermediaries be considered in the context of innovative solutions to invasions of online privacy, but that full consideration should be given to the potential for intermediaries to be subject to secondary liability for breaches of any proposed statutory tort. If intermediaries were to be held secondarily liable for breaches of a statutory cause of action, the Foundation notes that there may be a case for a qualified defence that would limit liability where an intermediary takes reasonable steps to prevent privacy breaches, or limit the harms arising from online breaches.

The Foundation notes that submissions by individual members will address further means by which serious invasions may be addressed in the digital era.

[11] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008), [11.21].
[12] Ibid. [11.22]-[11.23].
[13] Ibid. [11.25].

For further information please contact:

David Lindsay david.lindsay@privacy.org.au

Board Member
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au