Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

12 December 2014

Office of the Australian Information Commissioner

By email: Consultation@oaic.gov.au

Dear Director,

Re: Guide to Privacy Regulatory Action consultation

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

This submission by the Australian Privacy Foundation responds to the Consultation Paper – on the chapters released on the Guide to Privacy Regulatory Action.

The Foundation is the nation's premier civil society organisation concerned with privacy. It is a non-partisan body that draws on expertise regarding law, business, technologies and public administration. It has provided invited and independent advice to parliamentary inquiries, law reform commissions and other bodies over the past two decades.

General Comments

We do wish to express some concern about the consultation. The time given for the consultation was very short. We would a more reasonable consultation period of 30 days for consultations. We are also concerned that only part of the guide was released for consultation. As the Guide is a complete document it would be more appropriate to release the entire Guide for consultation at the one time.

The Foundation strongly contends that it is essential that the Privacy Commissioner is a very active regulator which must include strategic enforcement. The Guide and the Policy should be used to strengthen regulatory action and create a culture of this within the regulator.

Chapter 1; Introduction

No comment.

Chapter 3: data breach incidents and Commissioner initiated investigations

1. The APF has a number of concerns regarding Chapter 3.

Legislative framework

2. The APF acknowledges that the Office has resource and time limitations upon it when the discretion is exercised to investigate a complaint. Against that, as currently enacted, the Privacy Commissioner is effectively the regulatory gatekeeper in taking action to deal with interferences with personal information. Individuals can take action in relation to breaches of the Corporations Act as can the Australian Securities and Investment Commission ("ASIC"). They can also take action in relation to consumer related claims, as can the Australian Competition and Consumer Commission (the "ACCC"). In relation to interferences with privacy except for the use of section 98 of the Privacy Act, the Privacy Commissioner in effect retains the power and exercises sole discretion to take action in relation to interferences with personal information. In effect he is the gatekeeper. In the past that discretion has been exercised with too much restraint when exercised at all. The resulting perception is that regulation is light touch and the risk of enforcement low. The consequence has been both a loss for individuals in having complaints not investigated and a belief by organisations that there is no incentive to be compliant with the Privacy Act. It is the APF's view that compliance remains patchy and overall quite poor[1].

3. In that context, and as a matter of good public policy, the Privacy Commissioner should adopt a more determined and effective approach both as to when to undertake investigations and their conduct than proposed in the guide. The paragraph:

> " The Commissioner may commence an investigation without a complaint if the matter may involve an interference with the privacy of an individual and the Commissioner considers it desirable to investigate. Where the Commissioner investigates and is of the view that an interference with privacy has occurred, the Commissioner may take further privacy regulatory action."

tends to the anodyne. Beyond stating, when the reducing the paragraph to its essence, that the Privacy Commissioner has discretion to investigate, or not, and take regulatory action, or not, it has little practical meaning. The paragraph should include a stronger onus on the Privacy Commissioner to investigate and to take regulatory action when there is a breach. Such wording may be:

> " The Commissioner will commence an investigation without a complaint if the matter involves an interference with the privacy of an individual and there are no other significant countervailing factors which would preclude such an investigation being undertaken. Where the Commissioner investigates and is of the view that an interference with privacy has occurred, the presumption is that the Commissioner will, unless there are significant countervailing factors present, take further privacy regulatory action."

It is important for entities to understand that the Privacy Commissioner will exercise his powers to ensure there is compliance and proper regulation. If the Privacy Commissioner finds there is an interference with privacy of an individual the default position should be that he should investigate. And if the there is a basis to take action he should do so.

Triaging a data breach incident

[1] See for example *Companies not ready for privacy laws,* the Australian 1 December 2013 http://www.theaustralian.com.au/technology/companies-not-ready-for-privacy-laws/story-e6frgakx-1226782545881

4. There should be some precision in the use of triage. As used in the draft guide it means little, essentially that there are three categories of breach. Without precision as to what each category means the process is meaningless. In medicine, where the term originates, the process has meaning. For example a common triage categorization in hospitals is:

    - **red:** needs immediate attention - critical life-threatening injury or illness; transport first for medical help
    - **yellow:** serious injuries needing immediate attention.
    - **green:** less serious or minor injuries, non-life-threatening, delayed transport; will eventually need help but can wait for others.

    Even with the broadness of those definitions the above categories have real meaning. The triage system as described in the proposed guide is meaningless as to what the scope of each form of breach entails. As such it means what the Privacy Commissioner wants it to mean. That is of little benefit to anyone considering the guide. Such a definition should be found within the guide.

5. In addition to the factors set out, which are reasonable, a further factor should be words to the effect of:

    - whether there is a regulatory benefit in taking action to highlight the need for compliance, provide incentive for entities with similar issues to take remedial action or to alter cultural norms which are inconsistent with regulatory requirements.

    Effective regulators do factor in the need to inform the markets of practices and take assertive action publicly. Given the relatively early days of the amendments to the Privacy Act and the laxity in compliance taking action is as necessary as education and information provision.

Low severity data breach incidents

6. The problem with this section is the lack of precision in the language. What exactly is "low severity"? It means what the reader, or Privacy Commissioner, wants it to mean. There is no certitude. No assistance to anyone reading the guide. It provides no accountability of the Privacy Commissioner either. In short, it is of little utility. It should be redrafted to provide at least some general parameters of what is meant by a low severity data breach.

7. Notwithstanding the above fatal flaw in the drafting the paragraph should be amended to provide:

    > The Office will generally manage low severity data breach incidents by contacting the entity (respondent) by phone or email to:
    >
    > - seek confirmation of the circumstances of the breach, steps taken by the respondent to contain and respond to the breach, and any further information required
    > - determine the extent to which personal information has been the subject of interference and what, if any, steps are being taken to notify those persons whose information is affected
    > - provide information where appropriate, including copies or links to relevant Office resources such as the *Data breach notification: A guide to handling personal information security breaches* and *Guide to Information Security*
    >
    > The Office will assess the information gathered. The Privacy Commissioner will seek written confirmation of the steps taken to contain and respond to the breach. Provided that the respondent has co operated with the Privacy Commissioner and

provided full and frank disclosure of all information relating to the breach, in many cases, no further action will be necessary and the matter will be closed.

Medium severity data breach incidents

8. As with the low severity section what exactly does "medium security" mean. There is no point establishing a triage system when there is no parameters as what each category means.

9. If there is a medium severity data breach the presumption should be that some form of enforcement action is required. At minimum an enforceable undertaking must be obtained. Why shouldn't the proposed better practices required be made enforceable? If the breach is of medium severity then there should be ample scope for an enforceable undertaking. The dot point relating to enforceable undertaking should provide:

    - At any time, the Commissioner may seek an enforceable undertaking from the respondent under s 33E of the Privacy Act. Upon acceptance of those undertakings the Privacy Commissioner may close the matter save if there is a breach of those undertakings.

High severity data breach incidents

10. Absent an understanding of what "high severity" means this section is fundamentally flawed. If the distinction is to mean anything substantial then the presumption must be that a CII will be commenced.

Commissioner initiated investigations (CIIs)

11. The paragraph:

    > If the Commissioner forms the view that:
    >
    > - a high severity data breach matter, or
    > - any other matter brought to the attention of the Office
    >
    > may involve an act or practice by the respondent that constitutes an interference with the privacy of an individual, or a breach of APP 1, the Commissioner may decide to open a CII into the matter.

    is drafted in vague and general terms. If there is a high severity data breach the presumption should be that there is a CII. If the Privacy Commissioner has come to a view that there may be an interference with the privacy of an individual then there should be an investigation. To do otherwise is an abrogation of responsibility.

12. It is imprudent to take voluntary notification of a data breach incident or demonstration of steps taken to remedy the data breach into account as to whether to undertake an investigation. Those matters may be prudent for consideration on penalty and further action. They are not relevant considerations as to whether the Privacy Commissioner should investigate.

Considerations in opening a CII

13. The considerations should be amended to

(a) amend the paragraph:

- in the case of a data breach incident, whether:
  - that incident has been assessed as 'high severity'
  - the entity that experienced the data breach has voluntarily and promptly notified the Office
  - the entity has taken appropriate steps to respond to the data breach, and has cooperated with the Office in remedying any breach

to read:

- in the case of a data breach incident, whether that incident has been assessed as 'high severity'

(b) delete the sentence:

- whether the burden on the entity likely to arise from the Office conducting the CII is justified by the risk posed to the protection of personal information

This bespeaks a very unfortunate approach to regulation. If there is a basis for a CII then it should be undertaken. Pondering whether an entity will suffer a burden, which particulars are not provided or even alluded to in general terms, from responding to such an investigation is an irrelevant consideration. Burden is not defined. It is essentially a term that carries a multitude of meanings and no certitude. That is the antithesis of good regulation. On a practical level incorporating this factor will present a difficulty for the Commissioner, in determining what "burden" should mean, and an opportunity for the entity, in being imaginative in arguing what a burden does mean. It will prompt submissions from entities about "burdens". It is an irrelevant factor.

Chapter 4 Enforceable Undertakings

The Australian Privacy Foundation has a number of concerns regarding Chapter 4 as currently drafted. They are:

Enforceable undertaking terms and requirements

2. Section 33E is the point of reference for guidelines relating to enforceable undertakings. It provides:

(1) The Commissioner may accept any of the following undertakings:

(a) a written undertaking given by an entity that the entity will, in order to comply with this Act, take specified action;

(b) a written undertaking given by an entity that the entity will, in order to comply with this Act, refrain from taking specified action;

(c) a written undertaking given by an entity that the entity will take specified action directed towards ensuring that the entity does not do an act, or engage in a practice, in the future that interferes with the privacy of an individual.

(2) The undertaking must be expressed to be an undertaking under this section.

(3) The entity may withdraw or vary the undertaking at any time, but only with the consent of the Commissioner.

(4) The Commissioner may, by written notice given to the entity, cancel the undertaking.

(5) The Commissioner may publish the undertaking on the Commissioner's website.

3. In this context the guidelines should be amended as follows:

(a) The proposed sentence:

> In addition, the Office expects that the terms of any undertaking would usually (at a minimum):

should be amended to read as follows:

> In addition, the Office expects that the terms of any undertaking will, where applicable, include the following (at a minimum):

An enforceable undertaking is a legal document. It is important that the guidelines are expressed as precisely and specifically as possible. The terms should be as clearly expressed as possible. The term "usually" is vague. It begs the question when wouldn't some of the terms not be applicable. If the terms are applicable they should be applied. If they are not, they shouldn't.

(b) The term:

- be readily understood. For example, an undertaking that deals with complex and technical issues may have a glossary to define the terms used

This is not a term. It is an aspiration of very little import for the purpose of the, say, Privacy Act. The term "readily understood" has little meaning. What is readily understood to one person is not so to another. Having regard to the Privacy Act the issue for the Privacy Commissioner is not the readiness of an undertaking to be understood but whether it is enforceable for the purpose of section 33F which provides:

> (2) If the court is satisfied that the entity ***has breached the undertaking***, the court may make any or all of the following orders:
>
> (a) an order directing the entity ***to comply with the undertaking***;
>
> (b) any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or ***damage as a result of the breach***;
>
> (c) ***any other order that the court considers appropriate***.

There is no point obtaining an enforceable undertaking if it is not drafted in terms that are capable of enforceability. That may require complex terminology which may render the document not "readily understood" to a lay person. The term should be deleted.

(c) The term:

- describe the act(s) or practice(s) about which the Office is concerned

has no legal and very little practical meaning. The drafting is vague and non specific. That is not helpful for a practitioner considering the guidelines or the Privacy Commissioner in using them. The issue of what may "concern", whatever that means, the Privacy Commissioner is irrelevant. It is what may constitutes a contravention of an Act. It should be redrafted making reference to specific/specified act(s) or practice(s).

(d) The term:

- identify when and how the act or practice of concern was or is being rectified (unless it is incapable of being rectified)

should be amended to remove reference to "concern." Better drafting is "..specified act or practice". Why is it is necessary to refer to "was rectified" or "was being rectified" (depending on interpretation)? At first instance it is poor drafting. More importantly, it is not consistent with the terms of the, say, Privacy Act. The written undertaking under the Privacy Act refers to an undertaking:

(i) about future specified action that will be undertaken[2];
(ii) refrain from taking specified action in the future[3];
(iii) taking specified action in the future towards ensuring that it does not do an act or engage in a practice which interferes with privacy.[4]

There is no scope for prior rectification. This term should be amended.

(e) The term:

- contain a commitment to take necessary and proportionate action directed towards ensuring the act or practice of concern does not occur again

Again, the term "of concern" means little. Better drafting is "..specified act or practice". The question of proportionality is not a matter the Federal Court will consider. Given that is the case why should it be relevant as a guideline.

(f) The term:

- contain the respondent's agreement to material that arose in conciliation (if conciliation occurred) being submitted in any proceeding to enforce the undertaking. Where an undertaking forms parts of a conciliated outcome, this could be achieved by a statement of agreed facts being attached to the undertaking with the consent of both the respondent and complainant

is unnecessary. An undertaking is written for the purpose of, say, section 33E. Its existence is separate from any conciliation process even if it may arise subsequent to it. That is the four corners of any enforcement action. It is analogous to a Deed of settlement arrived at the end of a mediation. That document may have its genesis in discussions during a mediation but its enforceability is not reliant upon those discussions or documents produced during those discussions being made public. Under section 33(2) of the Privacy Act the Court is limited to making orders relating to a breach of the undertaking. The analysis in support of this term, footnote 5, is flawed.

(g) The term:

- include a compliance monitoring and reporting framework. The framework should include obligations for reporting to the Office (which may include a requirement for an independent expert to verify that specific steps have been taken or a particular issue rectified) and a requirement to nominate in writing a representative responsible for ensuring the establishment and operation of the framework

should be strengthened to read:

- include a compliance monitoring and reporting framework. The framework must include obligations for reporting to the Office (which may include a requirement for an independent expert to verify that specific steps have been taken or a particular issue rectified) and a requirement that the entity nominates in writing a representative

[2] Section 33E(1)(a)
[3] *Ibid* 33E(1)(b)
[4] *Ibid* 33E(1)(c)

responsible for ensuring the establishment and operation of the framework.

(h) The term:

- contain the respondent's acknowledgement that the Office may publish the undertaking in full (see 'Publication' below for further information). Any concerns the respondent has about publication should be raised and resolved as the terms of the undertaking are being negotiated.

Why is it necessary to obtain a respondent's acknowledgment that the Office may publish the undertaking? What specific legislative provision requires the Privacy Commissioner to require some form of acknowledgment as a term of the undertaking? It is not required for the purpose of enforcement. An undertaking is not *ipso facto* a confidential document. It should be published wherever possible. Enforceable undertakings not only relate to remedial action from the malefactor but send a message to the market that certain conduct is unacceptable. That is good public policy. Requiring some form of acknowledgment is poor public policy. Of course aspects of an enforceable undertaking may be anonymised or pseudonomised but that has nothing to do with the undertaking itself.

Negotiating the terms of the enforceable undertaking

4. The paragraph:

> " At the outset of negotiations, the Office will identify a reasonable time frame within which any undertaking should be negotiated. If an agreed undertaking cannot be negotiated within that time, the Office will consider pursuing alternative enforcement mechanisms in the matter such as proceeding to making a determination."

should be amended to provide:

> " At the outset of negotiations, the Office will identify wherever possible a reasonable time frame, having regard to the circumstances, within which any undertaking must be negotiated, the terms agreed as between the parties and a document provided to the Privacy Commissioner for final acceptance. If an agreed undertaking cannot be negotiated within that time, the Office reserves the right to pursuing alternative enforcement mechanisms without further notice."

A perennial and chronic problem in privacy regulation is the seemingly excessive delay between complaint, investigation and outcome. Wherever possible the guidelines should be drafted to require the Privacy Commissioner to act both reasonably and expeditiously.

Undertaking published

5. The paragraph:

> " Once the undertaking has been appropriately executed by both the respondent and the Commissioner, the Office may arrange for publication of the undertaking (see the 'Publication' heading below)."

should be amended to read as follows:

> " Once the undertaking has been executed by both the respondent and the Commissioner, the Office shall, unless there are legal or strong public policy issues to the contrary, publish the undertaking as soon as practicable."

6. The default position should be that enforceable undertakings are to be published. It is an effective means by which entities will understand their obligations and take note. It is good public policy for such documents to be made public. There is no prejudice to an entity having an enforceable undertaking made public. It is consistent with the practice adopted by the UK

Information Commissioner and the US Federal Trade Commission under their respective regulatory regimes.

7. Given the relatively poor compliance by entities with the Privacy Act it is good policy to ensure that enforceable undertakings are made public for the foreseeable future.

Ongoing monitoring

8. The paragraph:

> " It is the respondent's responsibility to ensure it complies with the terms of the undertaking and any compliance and reporting framework outlined in the undertaking. The Office will maintain contact with the respondent and monitor the respondent's compliance, including by ensuring that required reports and notifications are provided. If the respondent breaches the undertaking, the Office may take further action (see below)."

should be amended to provide:

> " It is the respondent's responsibility to ensure it complies with the terms of the undertaking and any compliance and reporting framework outlined in the undertaking. The Office will monitor the respondent's compliance. If the respondent breaches the undertaking, the Office will, unless there are good public policy or legal reasons to the contrary, take further action."

There is little point obtaining an enforceable undertaking and not contemplating enforcement action in the event of a breach. It is poor public policy. It gives rise to an expectation that the legislation will not be properly regulated. The proposed paragraph is drafted in anaemic terms. The Privacy Commissioner is a regulator. It is not for the office to make contact with an entity which has entered into an enforceable undertaking. If there is a breach the default position should be action. To do otherwise is a failure of regulation.

Breach of an enforceable undertaking

9. The process described in this section is anaemic and inimical to proper regulation of the legislation. The paragraph:

> " The Office will first bring the issue of suspected or actual non-compliance with the terms of the undertaking to the attention of the respondent and seek a response. This notification and response may be sufficient to resolve minor or inadvertent breaches. Where this is not the case, and depending on factors including the nature and length of non-compliance, the reason for non-compliance and any past non-compliance, the Office may initiate further negotiations with the respondent with a view to varying the terms of the undertaking.

is poorly drafted. What is a minor or inadvertent breach? If the undertaking is drafted properly and consistently with the terms of section 33E(1) why is it necessary to undertake a general, vague and legally meaningless process of considering factors which have little legal relevance with the ultimate possible outcome of varying the terms of the undertaking. This sends all the wrong signals. Why obtain an enforceable undertaking when the malefactor will know there is a chance of renegotiating if it becomes too hard? This constitutes an abrogation of regulatory responsibility and will do little to improve compliance. This paragraph should be deleted.

10. The paragraph

> " The Office may decide to address more significant non-compliance through the court enforcement mechanisms provided for under the

Privacy Act (s 33F) and the PCEHR Act (s 95). This process is outlined below."

is drafted in vague and almost meaningless terms. A regulator should have discretion but also must be required to properly exercise its powers under legislation. The paragraph should be strengthened to read:

" Where the Office is of the view, based on reasonable grounds, of a breach or non-compliance of an enforceable undertaking it will commence court enforcement action under the Privacy Act (s 33F) and the PCEHR Act (s 95) subject to its resourcing capabilities. This process is outlined below."

Publication

11. Undertakings should be published. The paragraph providing:

" Generally, the Office will publish an undertaking or a summary of an undertaking on its website <www.oaic.gov.au>. An undertaking will usually contain an acknowledgement from the respondent that the undertaking (or a summary) may be published, unless the Office has agreed otherwise with the respondent when the undertaking terms were being negotiated (see above). The Office may agree otherwise where it is inappropriate to publish all or part of an undertaking because of statutory secrecy provisions or for reasons of privacy, confidentiality, commercial sensitivity, security or privilege. In particular, due to the confidential nature of complaint investigations, it may be inappropriate to publish an undertaking accepted during a complaint process and to identify the respondent providing the undertaking. In such cases, the Office may publish a summary of the undertaking."

should be read to read as follows:

The Office will, unless there are legislative restrictions to the contrary, publish an undertaking or a summary of an undertaking on its website <www.oaic.gov.au>. The Office may agree to edit the undertaking for the for reasons of privacy, confidentiality, commercial sensitivity, security or privilege however will only do so to the extent required to address those issues."

12. An enforceable undertaking is not part of the complaints process. It is a stand alone procedure. A complaints process may result in discussions which may ultimately lead to an entity entering into an enforceable undertaking but the undertaking is separate from the process. It is a self contained document which should have no reference to the complaints process if drafted properly. Referring to the complaints process as a reason militating against publication makes no legal sense and is poor public policy. Given a respondent may be the subject of Federal Court action why should that entity not be named. That entity would be entitled, as of right, to be anonymised if such action is taken.

Chapter 7: Civil penalties – serious or repeated interference with privacy and other penalty provisions

Serious interference with privacy

1. In addition to the factors set out in considering whether a particular interference is serious should include:

- whether the senior or experienced personnel knew or should have known of the conduct and took no or no effective steps
- whether the conduct was motivated by or otherwise influenced by the prospect of financial gain or other form of advantage;

It is not sufficient to have regard to whether senior staff being responsible for the conduct. If they knew and willingly averted their eyes to egregious conduct or facilitated such an act but were not responsible in the legal sense of the word then such behavior should be relevant. Similarly breaches for monetary or business gain, which is a possibility, should be covered.

2. Given the need for active enforcement there should be a presumption of action in certain circumstances. The paragraph reading:

> " The Office will not seek a civil penalty in all matters involving a 'serious' interference with privacy. The Office is more likely to decide to seek a civil penalty in a particular matter where one of the following factors is present:

is quite general and vague. It lacks rigour. It should be redrafted to read:

> " While it will not seek a civil penalty in all matters involving a 'serious' interference with privacy the Office will, unless there are strong public policy reasons to the contrary, seek a civil penalty in a particular matter where one or more of the following factors is present:

Repeated interference with privacy

3. As with serious interferences with privacy there should be a presumption of action rather than a suggestion that it might take place in light of certain factors. Accordingly the paragraph reading:

> The Office will not seek a civil penalty in all matters involving repeated interference with privacy. The cases in which the Office is more likely to seek a civil penalty for repeated interference with privacy are those where:

Should be amended to read:

> " While it will not seek a civil penalty in all matters involving a repeated interference with privacy the Office will, unless there are strong public policy reasons to the contrary, seek a civil penalty in a particular matter where one or more of the following factors is present:

Publication

4. It is imperative that the Office publishes the identified information about civil penalty proceedings. There should be no reference to "generally" within this section. It should be mandatory unless there are compelling reasons to the contrary. The only practical reason should be a court order suppressing details or the judgment.

Chapter 8 – Privacy assessments

No comments.

Chapter 9 – Directing a privacy impact assessment

Purpose and key features of the PIA direction power

1. The paragraph, absent footnotes, providing:

> " The Office expects an entity to consider conducting a PIA and publishing the final report whenever an entity proposes to engage in an activity or function involving the handling of personal information. Where the Office becomes aware of a proposal which may have a significant impact on the privacy of individuals, the Office will generally recommend that an entity undertake a PIA. Considering and conducting a PIA are intrinsically linked to an entity's obligations under APP 1. Entities can obtain guidance on conducting PIAs from the *Guide to undertaking privacy impact assessments*.

should be strengthened to provide:

> " The Office expects an entity to consider conducting a PIA and publishing the final report whenever an entity proposes to engage in an activity or function involving the handling of personal information. Where the Office becomes aware of a proposal which may have a significant impact on the privacy of individuals, the Office will, unless there are strong public policy reasons to the contrary, recommend that an entity undertake a PIA….

2. The Commissioner is first and foremost a regulator. If an agency is intransigent then the Commissioner should not be required to undertake prolonged consultation and discussion. If a PIA is required and there is a failure to co-operate then the Commissioner should not be tentative about issuing a direction. As such the paragraphs providing:

> " An agency should not wait for a recommendation or direction from the Office to conduct a PIA. The Office expects agencies will recognise the benefits of conducting a PIA and a PIA direction should not generally be required. A PIA direction should be a last resort, where the Office considers that a PIA is necessary to ensure that an activity or function is appropriately balanced against the protection of the privacy of individuals and the agency is not already conducting a PIA.
>
> This is consistent with the Office's preferred regulatory approach of working with entities to facilitate legal and best practice compliance. To assist with this approach in relation to agencies, the Office will use the Information Contact Officer Network to ensure agencies maintain an open dialogue with the Office so that the Office is aware of major projects or policies that are being proposed and that may require a PIA.

are unnecessarily solicitous of an agency's possible concerns, real or otherwise. If PIA's are important, as they are, and the Privacy Commissioner believes they are appropriate in a situation then he should issue a direction without binding himself to a vague process which is more about relationship building than regulatory responsibility. Accordingly the paragraphs should be amended to provide:

> " An agency should not wait for a recommendation or direction from the Office to conduct a PIA. The Office expects agencies will recognise the benefits of conducting a PIA and a PIA direction should not generally be required. While a PIA direction is a serious regulatory action it will be made where the Office considers that it is necessary to ensure that an activity or function is appropriately balanced against the protection of the privacy of individuals and the agency is not already conducting a PIA.
>
> The Office will wherever possible work with entities to facilitate legal and best practice compliance. To assist with this approach in relation to agencies, the Office will use the Information Contact Officer Network to ensure agencies maintain an open dialogue with the Office so that the Office is aware of major

projects or policies that are being proposed and that may require a PIA. It will however make always reserve the right to make a PIA direction when the circumstances dictate.

Procedural steps in issuing a PIA direction

3. The APF believes that some amendment is required in the procedural steps. The paragraph providing:

- An agency may seek an extension of time in which to give the PIA to the Commissioner. The Office would generally grant an extension where:
  - the proposed function or activity will not be implemented during the time period of the extension
  - the extension will not otherwise impact the ability of the agency to adopt the recommendations in the PIA, or
  - the extension is otherwise reasonable in all the circumstances.

should be amended. If a PIA is required an extension should only be permissible where there is a compelling reason to do so. The paragraph should be amended to provide as follows:

- If an agency seeks an extension of time in which to give the PIA to the Commissioner the Office will only accede to the request if:
  - there is a legitimate and verifiable basis for that request;
  - the request does not relate to matters of convenience for the agency;
  - the proposed function or activity will not be implemented during the time period of the extension;
  - the extension will not impact the ability of the agency to adopt the recommendations in the PIA, and
  - the period of time in question is for the minimum period in all the circumstances the extension is otherwise reasonable in all the circumstances.

4. The paragraph providing:

- The Office will seek confirmation from the agency that the agency has implemented the recommendations in the PIA in accordance with the agency's responses to those recommendations prior to the implementation of the activity or function. Where the Office continues to hold concerns about the impact of a proposed activity or function on the privacy of individuals, the Office may inform the Minister of the matter.

Should be amended to provide:

- The Office will seek confirmation from the agency that the agency has implemented the recommendations in the PIA in accordance with the agency's responses to those recommendations prior to the implementation of the activity or function. Where the Office continues to hold concerns about the impact of a proposed activity or function on the privacy of individuals, the Office shall, unless there are strong public policy reasons to the contrary, inform the Minister of the matter.

Steps the Office will take where an agency does not comply with a direction

5. Compliance is a fundamentally important part of proper regulation. The proposed process set out by the guidelines is more consistent with the Privacy Commissioner working in the schedule of an agency rather than an agency undertaking its obligations. It is poor policy and even worse regulation. The paragraph providing:

> Where an agency does not comply with a PIA direction, the Office will use the following procedure:
>
> - If an agency has not complied with the PIA direction the Office will first contact the agency to determine the agency's progress and whether and when they intend to comply with the PIA direction.
> - If the agency does not intend to comply with the PIA direction within a reasonable timeframe, the Office is likely to consider this a failure to comply with the direction.
> - Where an agency has failed to comply with a PIA direction, the Office will advise both the Minister responsible for administering the Privacy Act, and the Minister responsible for the non-compliant agency (as required by s 33D(6)).

imposes upon the Office constraints and a process which makes little regulatory sense and seems to indicate tentativeness in fulfilling regulatory responsibilities. Why is it necessary to inquire as to whether an agency will comply with a PIA direction? It is a direction, not a suggestion. A failure to comply should bring consequences. The above procedure constitutes a failure to properly regulate. That has consequences for both the proper administration of the Privacy Act and the credibility of the Privacy Commissioner. The paragraph should be amended to provide:

> Where an agency does not comply with a PIA direction, or the agency informs the Office or otherwise makes clear that it does not intend to comply with the PIA direction within a reasonable timeframe the Office will advise both the Minister responsible for administering the Privacy Act, and the Minister responsible for the non-compliant agency (as required by s 33D(6)).

Publication

6. The default position should be that publication is mandatory and as much of a PIA direction should be published as possible. To that end the paragraph reading:

> " The Office will generally publish all PIA directions issued, and will require the agency to publish all final PIAs prepared in response to a PIA direction. To the extent possible, the Office will publish PIA directions in full or in an abridged version on its website: <www.oaic.gov.au>. It is sometimes inappropriate to publish all or part of a PIA direction or PIA because of statutory secrecy provisions or for reasons including privacy, confidentiality, commercial sensitivity, security or privilege. The Office will take those considerations into account when deciding whether to publish a PIA direction, and whether to require an agency to publish their PIA."

should be amended to read:

> " The Office will, unless there are binding legal or compelling public policy reasons to the contrary, publish all PIA directions issued, and will require the agency to publish all final PIAs prepared in response to a PIA direction. While it is sometimes inappropriate to publish part of a PIA direction or PIA because of statutory secrecy provisions or for reasons including privacy, confidentiality, commercial sensitivity, security or privilege the Office will

> only abridge or delete those portions of a PIA direction or PIA to the minimum extent possible so as to deal with the above constraints. The Office will publish PIA directions and final PIAs in full or in an abridged version on its website: <www.oaic.gov.au>."

The onus should always be upon publication. If deletions and abridgment is required the default position must be to delete and abridge with parsimony, not gusto.

Representatives of the Foundation would be pleased to discuss this submission with you and address particular aspects in more detail.

Thank you for your consideration.

Yours sincerely

Australian Privacy Foundation

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 AC CMG and The Hon Elizabeth Evatt AC, 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/