Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

4 March 2016

Commercial and Administrative Law Branch
Attorney-General's Department

By email: privacy.consultation@ag.gov.au

Re: Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

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

The Australian Privacy Foundation (The "Foundation") welcomes the prospect of a mandatory data breach notification Act but submits that there is considerable scope for improving the draft Bill.

The Foundations submission is set out as follows:

1. The Foundation's overall position
2. General Principles (pages 1-2)
3. Exposure Draft (pages 2-7)
4. Recommendations (pages 7-9)
5. Annexure 1: The Foundation's policy regarding Data breach notification

THE FOUNDATION'S OVERALL POSITION

The Foundation strongly endorses the establishment in national legislation of a mandatory data breach notification Act. There is a strong need for such legislation

The Foundation welcomes the enactment of Mandatory Data Breach Notification legislation. The Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 ("the NSDB Bill") goes some way to providing a structure for notification of data breaches. Unfortunately the NSDB Bill has structural defects and weaknesses which makes for a significantly less effective framework than it could be. This diminishes its likely effectiveness.

The Foundation recommends that the NSDB Bill be amended in line with the submissions made by the Foundation and set out in the recommendations.

GENERAL PRINCIPLES

Data breaches of personal information are becoming increasingly common. Personal information disclosed as a result of data breaches is becoming a reliable and lucrative source of income for criminal hackers. Such data may also be targeted by foreign government or quasi government authorities, or persons acting on their behalf. Consumer confidence in technologies such as the expansion of e-commerce and the broad use of personal information in health care, marketing and payment transactions is eroded by the prevalence of the egregious data breaches. Poor privacy training and data handling practices exacerbates this situation.

Information privacy is more than a consumer protection issue. It is a significant economic concern. A voluntary reporting scheme relating to the reporting of data is a poor regulatory model. In the main there is a poor privacy culture in Australia. This is, in large measure, a product of a prolonged period of weak legislation and weak regulation by successive Privacy Commissioners.

Without mandating the reporting of data breaches there is little incentive for organisations to alert individuals that their personal information has been accessed and potentially compromised. Without a proper reporting regime, organisations have little incentive to attend to their defective privacy protections. Without mandating the reporting of data breaches the temptation is all too often for an entity to contain the damage and avoid notifying the authorities and customers/clients.

The Foundation maintains that even with a satisfactory mandatory data breach notification regime, the limited scope and operation of the *Privacy* Act 1988 (The "Privacy Act") constitutes a fundamental flaw in regulation. That small business can be excluded from the operation of the Privacy Act is an ongoing failure of public policy. The other exemptions, such as employment information and personal information held by media and political parties compound this problem. The Foundation notes that problems with the coverage of the Privacy Act identified by the Australian Law Reform Commission in its 2008 report, *For Your Information,* have yet to be satisfactorily addressed by the government. The lack of broad coverage of the Privacy Act, including in relation to mandatory data breach notification provisions will, with time, cause both a regulatory problem and raise issues of fairness. Small businesses rely on the collection and use of personal information and are as prone to data breaches as businesses falling within the scope of the regime. That a small business operator should not be required to notify a client or customer of the misuse of his or her personal information while a slightly larger organisation must do so is inequitable. It may also lead to avoidable losses being suffered by an individual who is not notified.

THE EXPOSURE DRAFT OF THE BILL

The Foundation's concerns about the NSDB Bill are set out under the following headings.

Schedule 1

There is no good policy reason for a mandated delay in the operation of the breach notification provisions of the Privacy Act. It has already long been regarded as prudent practice to provide notification of the data breaches involving personal information. Organisations covered by the Act should be aware of their obligations under Australian Privacy Principle ("APP") 11. Those who avail themselves of the material on the homepage of the Office of the Australian Information Commissioner ("OAIC") should be aware of its guidelines about notification about data breaches, and that it is best practice to provide notice.

It should be a matter for the Privacy Commissioner to engage in any graduated approach to enforcement, if necessary, rather than delay the commencement of the legislation. That is likely to be the case in any event. The Privacy Commissioner has already prepared Guidance for a voluntary data breach notification. It should not require a year for his office to prepare for a mandatory data breach notification regime.

Organisations with a foreign presence, particularly those operating in the United States would be familiar with such a regime, usually more complicated than that being envisaged in this Bill.

Moreover, organisations who are compliant with their obligations under the Privacy Act now should have no difficulty in being able to comply with the data breach notification provisions.

The proposal to enact a mandatory data breach notification law has been the subject of public debate and reportage since 2013. There is therefore no reason for its operation being delayed.

Nomenclature – serious data breach/serious harm (clauses 26WB and 26WC)

In the Foundation's submission there is little merit in confining notification to incidents involving a serious data breach. A breach is significant if it entails the access to or the loss of personal information *per se*. As a matter of interpretation the term "serious data breach" and "serious harm" is confusing and lacks specificity.

A serious data breach is defined at clause 26WB(2) as involving some form of unauthorised access or disclosure which will "...result in a real risk of serious harm.." to individuals. A real risk is defined[1] as "..a risk that is not a remote risk." Harm is defined[2] as including:

(a) physical harm; and
(b) psychological harm; and
(c) emotional harm; and
(d) harm to reputation; and
(e) economic harm; and
(f) financial harm.

The breadth of harm is very broad, virtually covering the field in relation to the forms of harm an individual can suffer. What is less clear is how a reader of the statute can determine what amounts to "serious harm", which is presumably a sub set of the harm category.

Given there is a clear distinction drawn between "serious harm" and "harm" this is an extremely important threshold question for the operation of the scheme. There are no means within the Bill to distinguish between serious and other forms of harm. In practical terms what is the difference between harm and serious harm? The intent of this distinction seems to raise the threshold for reporting. What it is more likely to do is to create confusion as to where the threshold lies. Vaguely drafted and ambiguous terms such as this invariably reduce the effectiveness of the operative provisions when enacted.

There is no specific or even general provision within the Bill distinguishing one form of data breach, being serious, from another, being just a data breach. This presents a problem for entities required to comply with the regime, especially as there is an element of self reporting associated with the legislation, with the entity considering the relevant matters in Clause 26WB(3), giving its own weighting to each factor or a combination of factors and then determining whether it is obliged to report under clause 26WC. This is a flaw in the drafting. Any Guidance that may be produced by the Privacy Commissioner is just that. It is not a regulation or aid to statutory interpretation, and not a substitute for legislative clarity. In practical terms it is relevant to note that the Guidances prepared by the Privacy Commissioner are almost invariably drafted in broad and opaque terms. As such they are unlikely to remedy problems with legislative drafting.

Clause 26WB(3) is drafted in terms which provide ample scope for an entity to work on the basis that serious harm is a threshold which is sufficiently high to avoid reporting a data breach in many cases where the best practice, not to mention the intent of the legislature, would warrant notification. Without more certainty in the interpretation of "serious harm", and assuming such term remains (which the Foundation strongly submits should not be retained), it is possible, if not likely, that the mandatory data breach notification regime will be compromised.

The Foundation's policy is that the notification requirement should be based on either of the following conditions being satisfied:

(a) a risk of harm as opposed to the proposed "serious" risk; or

[1] At clause 26WG
[2] At clause 26WF

(b) a significant breach, whether or not a real risk of harm has arisen.

The Foundation recommends that the adjective "serious" be deleted from any reference to harm in the NSDB Bill.

Real risk of serious harm (Clause 26WB)

The relevant factors set out in Clause 26WB(3) in determining whether there is a real risk of serious harm to an individual are drafted in general terms. Given any assessment is to be undertaken by the entity affected by a data breach such an exercise is likely to favour an ostensibly plausible analysis resulting in a determination that that there was no real risk of serious harm, even where best practice might suggest that such risk is extant. The Explanatory Memorandum indicates that the inclusion of the "serious harm" category is to avoid the possibility "..that every data breach be subject to a notification requirement " and, accordingly, avoid notification fatigue. In the Foundation's submission the concern regarding over notification, with the associated cost, is more grounded in assertion and assumption than fact. The proposed solution in purporting to reduce instances of "minor" breach notifications by establishing a "serious harm" threshold is likely to have entirely the opposite outcome: under reporting. That is all the more likely given the poor privacy culture and ineffective regulation of the Privacy Act to date.

As drafted any analysis undertaken by an entity in the event of a serious data breach will almost certainly lack rigor given the inherent vagueness and generality of clause 26WB(3). Given there are no real objective standards in that assessment there will also be a lack of consistency in the manner in which entities will consider and apply the factors set out in clause 26WB(3)(at least until the Federal Court considers this provision). This predictable outcome is inimical to effective regulation relying heavily, as it does, upon judicial clarification to provide some form and substance to the operation of clause 26WB(3). That is unlikely to occur in the short to medium term, if at all. Accordingly, the clause should be revised.

The Foundation recommends that clause 26WB, in particular sub clause 26WB(3), should be redrafted to provide that the default regulatory starting position is the presumption of a real risk of (serious) harm in the event of a data breach, except where the entity can satisfactorily establish that the information cannot identify personal information or is in format where it is not intelligible to a person with advanced computer skills and it is not reasonably possible to be rendered intelligible. This would provide both greater certainty to the operation of the regime and better protection for victims of data breaches.

In relation to the current drafting of clause 26WB (3) there are several relevant factors which should not be included, or should at least be significantly modified, if the current structure is to be used. They are:

(a) "Security measures" referred to in paragraph (e). This is an opaque term which has an impermissibly broad meaning. It is not a defined term in the Privacy Act and has no legal meaning within the NDSB Bill. Moreover, security measures could be wholly inadequate, a likelihood in many data breach incidents, or inappropriate. For example a security measure, in the form of an anti-virus/malware software program, may constitute protection at a very basic level; however it may not be properly "patched" or otherwise kept up to date. It would therefore constitute protection against older malware but not against more recent versions. On a strict reading of the provision the personal information would, nevertheless, be "protected" by a security measure. Or at least that interpretation is arguable. The Foundation therefore recommends merging sub-clauses (e) and (f). It would also be prudent to specifically require that security measures are kept current and are in line with best practice

(b) Paragraph (g): a core tenet of the privacy principles is that an individual must be advised and consent given before that person's personal information is used for a purpose other than that for which it is collected. The contents of sub clause (g) operates contrary to this fundamental principle. If an unauthorised person obtains personal information, by one form of data breach or another, as a matter of general principle the starting point should always be that there is a real risk of serious harm. The Foundation appreciates that there may be a range of recipients who are in receipt of personal information arising out of a data breach

who are likely to have differing motivations, extending from criminal hackers to those innocent recipients who may have received an email in error, or even found a hard copy of personal information by chance. The potential for harm often depends upon the recipient and his/her motivations. This analysis should be reflected in more detail within sub paragraph (g). Accordingly, the sub-clause should be drafted in more specific terms clarifying what factors are relevant in the assessment of harm to a recipient. For example, it should not be difficult to draft a sub paragraph "factor" that distinguishes between circumstances involving a knowledge or reasonable belief that criminal conduct has occurred, on the one hand, and innocent mistake or receipt, on the other;

(c) The nature of any mitigation, as set out in paragraph (i), is open to abuse and confection. Steps to mitigate the harm should, in our submission, be undertaken as a matter of course. The starting and ending point is whether there is a real risk of (serious) harm at the time of the breach. Mitigation is, on this analysis, a relevant factor in any enforcement action that the Privacy Commissioner may choose to take and goes primarily to the question of remedies or penalties, not whether the breach should be notified. As drafted the provision may, and probably will, lead to an entity undertaking an artificial and potentially self-serving exercise so as to claim it is taking action to mitigate the damage, however ineffective that action may be, which may relegate the level of harm from "serious harm" to just "harm". The forms of mitigation set out in the sub clause lend themselves to abuse by an entity in undertaking an exercise so as to plausibly argue that the steps taken are sufficient to militate against notification. This potential for abuse is most apparent in paragraph 26WB(3)(i)(ii) with an entity developing steps that will be taken which are supposedly "likely to mitigate the harm", whatever that means. This provision promises to be a boon for lawyers and security experts brought in to develop future steps that "will be taken"; and may become the main basis to avoid the need for notification entirely.

Compliance issues (Clause 26WD)

It is incongruous that a breach of the notification requirements under clauses 26WC, in particular, or 26WD is only an interference with the privacy of an individual[3]. If there is a failure to comply with the provisions relating to a ***serious data breach*** the Foundation submits that it should be regarded as a ***serious interference with the privacy*** of an individual under section 13G(1) of the Privacy Act. If the legislature chooses to set the bar high, requiring notification for a "serious" data breach, why should a breach of the notification regime not be regarded as a serious interference with privacy?

Furthermore, the Privacy Commissioner should have the option of commencing civil penalty proceedings arising out of a breach of clauses 26WC or 26WD if, in the exercise of his discretion, he believes that it is appropriate and the evidence warrants it.

As drafted a breach of clauses 26WC and 26WD is an "interference with privacy". An interference with privacy is a defined term. It does not give rise to a basis for a civil proceedings action by the Privacy Commissioner. In the context of mandatory data breach notification provisions it is unlikely that a failure to comply with providing a statement, notifying individuals or publish notice, would constitute such behaviour as to fall within an act or practice constituting a serious interference with privacy for the purpose of section 13G(a). It is highly unlikely that section 13G(b) would relate to a potential breach of a notification provision. It is arguable that the legislature, as the Bill is currently drafted, intended that a breach of clauses 26WC or 26WD to be limited to an interference with privacy only. If the Bill is enacted in its current form it would be difficult for the Privacy Commissioner to commence civil penalty proceedings in the event of a breach of clauses 26WC or 26WD even if the circumstances would warrant it from a policy perspective. .

As such the Foundation recommends that a serious data breach should constitute a serious interference with privacy. This could be enacted as a stand-alone provision or, alternatively, through an amendment to section 13G, in the form of inserting a new sub-section 13G(c), providing that a breach of clauses 26WC and/or 26WD constitutes a serious interference with the privacy of one or more individuals.

[3] Pursuant to clause 13(4A) of the Bill.

Exceptions to notification

The Foundation submits that there should be a minimum of exceptions to notification. The Foundation's policy is that the starting point should be that limited discretion should be given to the Privacy Commissioner in relation to the operation of a data breach notification regime. Any exemptions should therefore be minimal and specify the precise circumstances in which they are available.

Enforcement agencies should be required to specify to the Privacy Commissioner why compliance with the notice provisions would prejudice enforcement related activities. The relative *carte blanche* given to enforcement agencies regarding compliance in clauses 26WC(5) and 26WD(6) is poor public policy. A "belief on reasonable grounds" test is not sufficiently strong. Enforcement agencies are notorious in their poor data handling practices. The Privacy Commissioner should have the right to consider the reasons given and to challenge them if necessary. It is entirely possible, if not likely, that enforcement agencies may rely on the exemption in the draft Bill to protect their reputation rather than genuine concerns over prejudice to an ongoing investigation. In short, a certificate based entirely on self-certification is a poor substitute for proper substantiation. Similarly clauses 26WC(12) and 26WD(7) should be amended. The agencies should be required to apply for an exemption and affirmatively establish that there is a likelihood that compliance will materially and irreparably prejudice an activity. The Privacy Commissioner should have a power to reject the exemption.

Sub clause 26WC(14), which establishes an exception carries out a reasonable assessment and, as a result, reasonably believes there has been no serious data breach, should be deleted. As currently drafted it is open to abuse by regulated entities. It will likely be a boon for security experts, or those who describe themselves as such, as *ex post facto* reports provide a plausible rationale to downgrade the nature of the breach after the fact. "Reasonable grounds" in an area where there is so little established law, few regulations to provide objective measures, poor understanding of privacy best practice and little accountability can encompass a wide range of situations. It is a provision primed for abuse.

Action by affected individuals

Given data breaches can involve a cost to a victim, individuals should have a right to take action in the event of a breach resulting in harm or loss and damage. The Privacy Act should be amended to provide for an actionable cause of action arising out of a data breach. That right should be independent of any action that the Privacy Commissioner may take and not be conditional on any such action. Moreover, as data breaches may affect a large number of people, individuals should have a right to bring a class action where a large class has been affected. The benefits of a class action lawsuit is that it provides recovery to individuals who otherwise may not be able to afford legal fees while simultaneously incentivizing businesses to maintain proper data security standards.

Notification by OAIC

All actions arising out of a breach of mandatory data breach notification provisions should be posted on the OAIC web site. That should be done as a matter of course. It should be mandated by legislation. There should be an option to anonymise a party; however that should only be done where there are strong public policy grounds for doing so.

The Office of the Australian Information Commissioner should require that any notification made by an entity should be placed on its website and kept there indefinitely. There are strong public policy reasons for this, including:

(a) it is important to understand the extent to which reportable data breaches are occurring;
(b) the record of data breaches, and which entities have suffered them, should be a publicly known fact; and
(c) transparency in data breach notifications is likely to have a deterrent effect and this is desirable.

The cost implications of compliance with this policy are negligible for entities because they would already be required to provide a copy of the notifications to be published to the Commissioner; and the cost of web republication by the Commissioner is likewise negligible.

Responsibilities of the Privacy Commissioner

The Foundation recommends that the Bill be amended to include a section requiring the Privacy Commissioner to have general monitoring related functions in relation to personal information held by entities. The model for the provision should be section 28A of the Privacy Act, sub section 28A(1) in particular.

RECOMMENDATIONS

The Foundation supports the enactment of the NSDB Bill with appropriate amendments. It recommends:

Recommendation 1

Clause 2 of the Bill should be amended to delete the following:

> However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.

There is an urgent need for a data breach notification regime; and the case for a 12 month delay in implementing the regime has not been made out.

Recommendation 2

The adjective "serious" should be deleted wherever it appears to describe "harm" in clause 26WB. The requirement that there be a real risk of harm provides sufficient safeguard against notification fatigue.

Recommendation 3

Clause 26WB(3) should be redrafted so as to provide that the default position for an entity is notification unless it can establish categorically, and/or appropriately satisfy the Privacy Commissioner, that the personal information that has been lost, accessed or misused cannot identify a person, or is in a format where it is not intelligible to a person with advanced computer skills and it is not reasonably possible to be rendered intelligible.

Recommendation 4

If the legislature does not redraft clause 26WB(3) as recommended above it should:

(a) delete clause 26WB(3)(e);
(b) amend clause 26WB(3)(g), so that it is more specific as to what weighting should be given to the relevance of the recipient of the personal information in determining whether to consider there is a real risk of serious harm; and
(c) delete clause 26WB(3)(i).

Recommendation 5

Amend the *Privacy Act 1988* (Cth) to insert a new section 13G(c) to provide that a breach of clauses 26WC and 26WD amounts to a serious interference with privacy.

Recommendation 6

Amend clauses 26WC(5) and 26WD(6) to require agencies to apply for an exemption and to establish that there is a likelihood that compliance will materially and irreparably prejudice an activity or investigation. The Privacy Commissioner should have a power to reject the application.

Recommendation 7

Delete clause 26WC(14).

Recommendation 8

Insert a new provision in the *Privacy Act 1988* (Cth) to permit individuals affected by a serious data breach to have a cause of action arising out of any loss and damage they have suffered as a result of that data breach that is independent of any action taken by the Privacy Commissioner.

Recommendation 9

Insert a new provision in the *Privacy Act 1988* (Cth) requiring all notifications to be placed online by the Privacy Commissioner, and anonymised where necessary.

Recommendation 10

Insert a new provision in the *Privacy Act 1988* (Cth) conferring general monitoring related functions on the Commissioner in relation to data breaches. The model for the provision should be section 28A of the Privacy Act, sub section 28A(1) in particular.

For further information please contact: Peter Clarke on (03) 9225 8751.

Thank you for your consideration.

Yours sincerely



Kat Lane, Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay, Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile, Vice-Chair
0414 731 249
David.Vaile@privacy.org.au

APPENDIX 1

THE AUSTRALIAN PRIVACY FOUNDATION POLICY POSITION REGARDING MANDATORY DATA BREACH NOTIFICATION

A data breach occurs when personal data is exposed to an unauthorised person. It is a breach of trust by the organisation. It is commonly also a breach of the law. Unfortunately breaches of data protection laws are seldom subject to enforcement actions.

Data breaches occur remarkably frequently. Parliaments have failed to impose meaningful sanctions, and privacy oversight agencies have failed to exercise such powers and influence as they have to force organisations to ensure that appropriate security safeguards are in place.

In 2003, the Californian legislature responded to inadequacies in organisational practices by passing a Security Breach Notification Law. By 2006, 33 other US States had passed similar laws. Australian law reform has moved at glacial pace, and lags the US in this matter by a decade.

Definitions

A **Data Breach** occurs where personal data held by an organisation has been subject to, or is reasonably likely to have been subject to, unauthorised access, disclosure, acquisition or loss.

A **Serious Data Breach** is a Data Breach that gives rise to a reasonable risk of harm to an individual. A **Data Breach Notification** is a statement of the facts relating to a Data Breach.

The Purposes of Data Breach Notification

The purposes of Data Breach Notification are:

1. to inform the public, at a meaningful level of detail, about:
   - breaches
   - inadequacies in organisations' security safeguards
2. to inform individuals who have been affected by breaches, so that they can judge whether to:
   - take action to prevent or mitigate potential harm arising from the breach
   - seek compensation for harm caused
   - change their service-providers
3. to shame organisations that have seriously inadequate security safeguards into changing their ways
4. to encourage all organisations to implement adequate security safeguards

Data breach notification processes, guidelines and regulations need to be designed so as to achieve these purposes.

Organisations' Obligations in Relation to Data Security

1. All organisations must ensure that personal data is at all times subject to security safeguards commensurate with the sensitivity of the data. The Foundation has previously published a Policy Statement on Information Security
   - All organisations must take the steps appropriate in their particular circumstances to
   - deter Data Breaches
   - prevent Data Breaches
   - mitigate harm arising from Data Breaches; and
   - enable their investigation
2. All organisations must implement awareness, training and control measures to ensure appropriate practices by their staff
3. All organisations must conduct audits of security safeguards periodically, and when the circumstances warrant
4. All organisations must perform a Privacy Impact Assessment (PIA) when data systems are in the process of being created, and when such systems are being materially changed, in order to ensure that appropriate data protections are designed into their systems, and to demonstrate publicly that this is the case

Organisations' Obligations in Relation to Data Breach Notification

1. Conduct of an Investigation

Where grounds exist for suspecting that a Data Breach may have occurred, the organisation must conduct an investigation, in order to establish a sufficient understanding of the circumstances and the outcomes. The results of the investigation must be documented in a form that enables subsequent evaluation.

2. Submission of a Data Breach Notification

Where a Data Breach has occurred, or is reasonably likely to have occurred, the organisation must:

1. Submit a Data Breach Notification to the relevant oversight agency, in a manner consistent with the guidance issued by that oversight agency, as soon as practicable and without delay; and
2. Communicate sufficient information to affected categories of individual, the media, and/or representative and advocacy agencies, as appropriate to the circumstances

3. Form of a Data Breach Notification

A Data Breach Notification must include sufficient detail to enable the reader to achieve a proper understanding of the Data Breach, its causes, its scale, its consequences, mitigation measures, and the rights of individuals affected by it.

Details whose publication might result in harm or facilitate attacks on that or other organisations can be included within a separate Appendix whose distribution can be limited.

4. Additional Obligations in the Case of a Serious Data Breach

Where a Serious Data Breach has occurred, or is reasonably likely to have occurred, the organisation must, in addition:

1. Provide an explanation, apology and advice to each individual whose data is, or is reasonably likely to be, the subject of the Data Breach, as soon as feasible and without delay, but taking into account the possible need for a brief delay in the event that criminal investigation activities require a breathing-space
2. Publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information
3. Where material harm has occurred, provide appropriate restitution
4. Inform the oversight agency of the actions taken

5. The Responsibilities of the Oversight Agency

1. Publish guidance in relation to data security safeguards. This must make clear that organisations have obligations to perform Security Risk Assessment, and to establish an Information Security Risk Management Plan whereby information security safeguards are implemented and maintained, commensurate with the sensitivity of the data.
2. Publish clear and specific guidance in relation to Data Breach Notifications.
3. In relation to Data Breaches:
   - Liaise with organisations that have suffered Data Breaches
   - Facilitate the Submission of Data Breach Notifications
   - Inform the Public
   - Publish the Data Breach Notifications in a Public Register
4. In relation to Serious Data Breaches:
   - Review the outcomes of the organisation's internal investigation
   - Where doubt exists about the quality of the internal investigation, conduct its own independent investigation
   - Publish the results of the review and/or investigation
   - Add details of the investigation into the Public Register
5. Facilitate improvements in organisational practices relating to data security
6. Facilitate remedies for individuals who have suffered as a result of Data Breaches

6. Enforcement

All obligations in relation to Data Breach Notification must be subject to sanctions and enforcement.

The sanctions applied must reflect:

- the organisation's degree of culpability, including:
  1. the extent to which the organisation had implemented safeguards commensurate with the sensitivity of the data
  2. the extent to which the threat(s) and vulnerability/ies that gave rise to the Data Breach were well-known or novel
- the promptness and effectiveness with which the organisation reacted once grounds existed for suspecting that a Data Breach may have occurred

- mitigation measures adopted by the organisation once it was apparent that a Data Breach had occurred, or was reasonably likely to have occurred
- any avoidance activities, misinformation or delays by the organisation in responding to the Data Breach and in its interactions with the oversight agency
- the scale of the Data Breach
- the sensitivity of the data that was the subject of the Data Breach
- the measures undertaken by the organisation in order to address the risk of recurrence of Data Breaches (as distinct from the organisation's statements about what it intends to do)
- to the extent that financial penalties are applied, the size of the organisation

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 are 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/