Electronic Frontiers
AUSTRALIA

PO Box 1302, Kensington VIC 3031
T +61 3 9013 9492 F +61 3 9013 9468
E email@efa.org.au W www.efa.org.au
ABN 35 050 159 188

Mr Richard Glenn
Assistant Secretary
Business and Information Law Branch
Attorney-General's Department

Via email to: Privacy.Consultation@ag.gov.au

23rd November 2012

Dear Assistant Secretary,

Thank you for providing the opportunity to make a submission in relation to the Discussion Paper on the issue of Privacy Breach Notification.

Electronic Frontiers Australia Inc. (EFA) is a national non-profit organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (S.A.) in May 1994. Our website address is: www.efa.org.au.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer-based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities.

EFA has presented written and oral testimony to State and Federal Parliamentary Committee and government agency inquiries into regulation of the Internet and online issues.

Please find following our responses to the questions posed in the Discussion Paper. EFA would be pleased to expand on the issues below in oral testimony or otherwise.

Yours faithfully,

David Cake, Chairperson
On behalf of the Board, Electronic Frontiers Australia, Inc.

Electronic Frontiers AUSTRALIA

EFA Submission in relation to Australian Privacy Breach Notification

This submission references the Commonwealth Government's Discussion Paper: Australian Privacy Breach Notification, relating to the possible introduction of mandatory data breach notification laws.

The Discussion Paper defines mandatory data breach notification as a legal requirement imposed on particular entities to provide notice to affected persons and the relevant regulator where certain types of personal information are accessed, obtained, used, disclosed to, copied, or modified by unauthorised persons. Such unauthorised access may occur following a malicious breach of the secure storage and handling of that information (eg, a hacker attack), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise.

1. Should Australia introduce a mandatory data breach notification law?

1.1 Are the current voluntary data breach notification arrangements sufficient?

EFA does not believe that the current voluntary data breach notification arrangements are sufficient.

The announcement by the Office of the Australian Information Commissioner (OIAC) on 30th April 2012 demonstrates this point quite clearly. This announcement notes that the OAIC received notifications about 56 data breaches in the previous financial year, while a further 59 investigations had been opened in relation to suspected, but unreported, data breaches in the same period.[1]

It is reasonable to assume that there will have been additional unreported breaches, so it is therefore also reasonable to conclude that only a minority of data breaches are currently being notified to the OAIC, let alone to the affected individuals.

1.2 Should the Government introduce a mandatory data breach notification law?

EFA is very strongly supportive of the introduction of a mandatory data breach notification law, for the following reasons:

- it is clear, as noted above, that a voluntary regime is not sufficient to ensure that the majority of breaches are notified;
- data breaches can have very significant consequences for the individuals affected, including creating the potential for identity theft, breach of privacy and reputational damage;
- a mandatory notification regime would create a very strong incentive for organisations to take data security more seriously than many appear currently to do; and,

[1] http://www.oaic.gov.au/news/media_releases/media_release_120430_business-warned-to-be-ready.html

- a mandatory notification regime would also raise awareness among individuals about the need for them to treat their own data security and privacy as very serious issues and to take appropriate steps to protect themselves.

EFA rejects the following arguments against a mandatory data breach notification regime that are set out in the Discussion Paper.

The additional costs of compliance for entities would be too onerous

The costs involved in providing a notification about a data breach need not be significant, let alone onerous. Notification to the OAIC could involve little more than a web form submission, or email. Notification to affected individuals could similarly involve an email or physical letter, depending on the contact details held by the organisation.

Further, any organisation that believes that notifying their customers, members or other stakeholders that their data has been breached is too costly a burden for them to bear, arguably does not deserve to maintain the trust of those individuals.

In the paper published in 2010 by IT security firm Symantec (and cited in the Discussion Paper), it is noted that '[c]ustomer turnover in direct response to breaches remains the main driver of data breach cost.'[2] This conclusion reinforces the point that it is not notification of data breaches, but rather a lack of sufficient regard for data security, resulting in such breaches, that drives costs for organisations in this regard. It is evidently good business practice for organisations to give data security sufficient priority to minimise the likelihood of data breaches.

There are sufficient commercial incentives for entities (eg reputation) to have high standards of data security and to voluntarily notify the OAIC where appropriate

As noted above, it is clear that there simply aren't sufficient commercial incentives for entities to have high standards of data security and to voluntarily notify the OAIC. On the contrary, as the Symantec report referred to above makes clear, there are in fact strong commercial incentives, particularly in relation to reputation and customer retention, for entities to **not** report data breaches. As the OAIC statistics also referenced above also make clear, at present a minority of data breaches are currently being notified.

Many organisations do not have the capability of detecting whether data loss has occurred, and whether there has been a significant impact or harm caused by such data loss

Appropriate data security processes and mechanisms should include the ability to detect loss of data, however EFA acknowledges that different organisations will inevitably have different levels of sophistication in this regard, that should be related to the size of the organisation and the sensitivity of the data that they are collecting.

[2] http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf, page 6.

EFA therefore believes that the focus of mandatory data breach notification legislation should be on the notification of breaches, once they become known, rather than on overly prescriptive regulations about the mechanisms through which such breaches could be identified.

EFA recognises that there is a balance that needs to be found in this regard, between creating a perverse incentive for organisations to be willingly ignorant of data breaches, so as to avoid the requirement of notification, and the promotion of appropriate data security mechanisms and processes. As noted above in relation to the assertion that mandatory data breach notification would impose onerous costs on organisations, EFA reasserts the point that good data security is good business practice.

The connection between data breaches and identity theft has been criticised as being overstated

The paper by Romanosky et. al., referenced in the Discussion Paper states that '[i]dentity theft resulted in corporate and consumer losses of $56 billion dollars in 2005, with about 30% of known identity thefts caused by corporate data breaches.'[3] EFA believes that this demonstrates a very clear and significant connection between data breaches and identity theft.

Data breach disclosure laws have marginal effect on the incidences of identity thefts

The Romanosky paper also asserts that 'adoption of data breach disclosure laws have marginal effect on the incidences of identity thefts and reduce the rate by just under 2%, on average.'[4] EFA asserts that while the effect of such laws on the incidence of identity theft may have been seen to be marginal to date, that the effect of such laws is likely to increase over time as organisations and individuals become more conscious of data security, and also that identity theft is only one aspect of the harms that are associated with data breaches. Loss of privacy and other associated harms, including reputational damage, that can also result from data breaches are also important considerations.

2. Which breaches should be reported? Triggers for notification?

2.1 What should be the appropriate test to determine the trigger for notification?

EFA does not support the use of quantitative parameters as part of the trigger test for notification, as such tests are inevitably more focused on the cost to the organisation, rather than the potential for harm to individuals. EFA believes that the potential for harm to individuals should be the primary factor in determining whether notification is required.

As an example, should the files of a handful of individuals of a small-scale drug rehabilitation centre be breached, the potential for harm to those individuals would be immense, potentially even life-threatening. Any quantitative measure based on either the scale of the organisation, or the scale of the breach would likely exempt such an organisation from notification requirements.

[3] http://weis2008.econinfosec.org/papers/Romanosky.pdf, page 1.
[4] *Ibid*., page 1.

EFA believes that the proposal included in Senator Stott-Despoja's private members bill of 2007 (option 'g' in the Discussion Paper) provides the most appropriate test for determining the trigger for notification, ie that 'disclosure to unauthorised persons has occurred or is reasonably suspected to have occurred.'

EFA supports this test as it avoids making any value judgement about whether a particular individual's privacy has or may have been compromised, and provides a clearly-defined trigger for notification.

2.2 Should it be based on a catch all test, or based on more specific triggers, or another test?

See above.

2.3 What specific elements should be included in the notification trigger?

In many cases, the simple fact of having accessed a service, or interacted with an organisation, is enough information that its breach could lead to significant harm to an individual, and should therefore be included in the notification trigger. Obvious examples would include a drug treatment centre, Alcoholics Anonymous, domestic violence support groups and the like.

All core data elements should be included in the notification trigger, including , data elements such as birthdate, mother's maiden name, password, bank account details, credit/debit card details, drivers licence number, passport number.

Organisations that collect sensitive data elements should have additional data elements included in their notification triggers, which should be determined based on sector-specific guidelines that could be drawn up in consultation with OAIC.

3. Who should decide on whether to notify?

EFA believes that notification to the OAIC should be mandatory in all cases, and that notification to affected users should also be mandatory. There may however be instances in which certain organisations (such as law enforcement) may have legitimate reasons for not wanting to also notify affected users, or to have the breach publicised in any way. Such circumstances should be clearly specified in any legislation and should require the organisation involved to apply to the OAIC for an exemption from user notification for each breach. Commercial interests (including commercial confidentiality) or the type of an organisation (for example, political parties), should not be valid grounds for exemption from notification.

3.1 Who should be notified about the breach?

See above.

3.2 Which of the below should decide whether to notify?

i. the organisation or agency;

ii. the Commissioner; or

iii. the organisation/agency in consultation with the Commissioner

EFA believes that notification to the OAIC should be mandatory, in all circumstances. In circumstances where there may be a legitimate reason not to also notify affected users, that decision should be made by the OAIC, based on submissions from the organisation that has suffered the breach and subject to specified public and individual interest considerations.

4. What should be reported (content and method of notification), and in what time frame?

4.1 What should be the form or medium in which the data breach notification is provided?

Notifications should be provided to affected individuals using whatever is the normal form of communication between the organisation and its users. In the majority of cases, that is likely to be via email. Notification to the OAIC should occur through a carefully designed web-form submission process.

4.2 Should there be a set time limit for notification or a test based on notifying as soon as is practicable or reasonable?

EFA believes that notifications should be made as soon after discovery of a data breach as possible. This is particularly important where credit card or other personally sensitive information has been breached.

As a minimum, EFA believes that 28 days should be the maximum time limit for notifications.

4.3 What should be the content of the notification?

Notifications should include the following information:

- the nature of the data that has been breached – ie the database field names;
- the date and time on which the breach occurred;
- the potential impact of the breach of this data;
- the scale of the breach – eg was the entire customer base affected, or only users of one product;
- why the breach occurred – eg was it due to out of date software, or human error; and,
- links to relevant websites, including the OAIC and other sites that contain information about how to remediate a data breach and how to protect personal data to minimise the likelihood of further data breaches.

5. What should be the penalty for failing to notify when required to do so?

5.1 Should there by a penalty or sanction for failing to comply with a legislative requirement to notify?

EFA believes that to be effective, a mandatory data breach notification law must include financial penalties for non-compliance. Non-compliant organisations should also be included on a list to

be published on a regular (perhaps quarterly) basis. The combination of financial and reputational penalties should create powerful incentives for compliance.

5.2 If so, what should be the penalty or sanction, and the appropriate level of that penalty or sanction?

EFA believes that financial penalties should be relative to the turnover and assets of the organisation. A $1 million fine for a major corporation, for example, is likely to be completely ineffective in many instances, especially where the cost of compliance may be significantly higher. A $1 million penalty could of course however bankrupt many smaller organisations.

6. Who should be subject to a mandatory data breach notification law?

EFA believes that all public sector entities, including Commonwealth, State and Local Governments and their agencies should be subject to a mandatory data breach notification law. EFA also believes that as many private sector entities as practical should also be subject to such a law. EFA does however understand that it may not be practical to enforce a mandatory data breach notification law on every small business and small organisation. There are however many small entities that collect extremely sensitive information. EFA recommends that regulations governing which organisations should be subject to a mandatory data breach notification law should focus on the nature of the information being stored, rather than the size of the organisation.

7. Should there be an exception for law enforcement activities?

7.1 Should there be an exception for law enforcement activities?

EFA understands that there are circumstances in which the public interest may not be best served by the notification of data breaches relating to law enforcement activities. EFA believes however that the OAIC should be notified in all circumstances, and that there should be specified conditions under which law enforcement agencies could apply to the OAIC for the suppression of such notifications and for associated exemptions from the requirement to notify affected individuals.

7.2 Would such an exception add anything to the ALRC's proposed public interest exception?

EFA believes that the OAIC should apply a public interest test when assessing any such application for suppression of notification, or exemption from the requirement to notify affected individuals.