Electronic Frontiers
AUSTRALIA

Mail GPO Box 1235, Canberra ACT 2601
Phone 02 6101 9968 Twitter @efa_oz
Web www.efa.org.au Email email@efa.org.au

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit, Barton ACT 2600

Via email to: privacy.consultation@ag.gov.au

7th March 2016

Re: Serious Data Breach Notification Consultation

Dear Sir/Madam,

Electronic Frontiers Australia (EFA) appreciates the opportunity to provide this submission in relation to this consultation. EFA's submission is contained in the following pages. EFA is happy to provide further information, if required.

This submission is not confidential and is intended to be made public, in full.

About EFA

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights.

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 civil liberties in the digital context. 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 digital 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 digital communications systems.

Yours sincerely,

[redacted]

Jon Lawrence
Executive Officer, on behalf of EFA's Policy Team

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

Electronic Frontiers AUSTRALIA

Submission to the Serious Data Breach Notification Consultation

1. Introduction

EFA has long been a supporter of the introduction of legislation requiring notification of data breaches involving personal data. EFA notes that this is at least the fourth iteration of such legislation to be drafted since the Australian Law Reform Commission's August 2008 report, For Your Information: Australian Privacy Law and Practice, which recommended the introduction of a mandatory data breach notification scheme.[i]

EFA also notes the recommendation of the Parliamentary Joint Committee on Intelligence and Security in February 2015 that a mandatory data breach notification scheme be implemented before the end of 2015[ii], and the commitment made by the Attorney-General on 3rd March 2015 to comply with this recommendation.[iii]

EFA also notes the undue haste and clear lack of sufficient consultation with the full range of stakeholders involved in both the drafting and legislative processes for the introduction of related legislation, such as the [TIA Amendment] which introduced a mandatory retention regime for telecommunications data.

The very serious issues that are being encountered in the implementation planning process for the mandatory telecommunications data retention regime highlight the dangers of such undue haste and lack of consultation. The data retention legislation is clearly fundamentally flawed and in need of urgent review, less than one year after its passage through the parliament.

In contrast, this draft legislation has evolved through a number of iterations over a number of years with multiple public consultations. EFA therefore looks forward to the introduction and passage of this legislation without further delay.

EFA also believes there is no justification whatsoever for a 12 month delay in the commencement of the mandatory notification requirement following Royal Assent.

1.1 Statutory cause of action

EFA strongly supports, in principle, the establishment of a statutory cause of action for serious invasions of privacy, such as that outlined in the Australian Law Reform Commission's report, tabled in parliament on 3rd September 2014.[iv]

The creation of a potential civil remedy for individuals affected by serious invasions of privacy will be an important additional protection for the privacy of all Australians.

It should be noted that committees of both the NSW[v] and Victorian[vi] parliaments have recommended the introduction of such a statutory cause of action, and the Australian Law Reform Commission set out a model for the same in a report released in March 2014[vii].

Given the relative urgency of implementing a mandatory data breach notification scheme, it is assumed that it will not be possible for a general statutory cause of action for breach of privacy to be legislated in parallel.

EFA therefore recommends the inclusion of a specific statutory cause of action relating to data breaches falling within the remit of this legislation.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

2. General Comments

Mandatory data breach notification is an important addition to Australia's privacy protection regime which EFA believes will provide an additional impetus for privacy and data security to be regarded as a critical organisational risk factor requiring attention at the highest levels of management among Australian organisations. It is particularly critical in the context of the mandatory retention regime for telecommunications data that came into effect in October 2015.

It is suspected that many organisations have avoided disclosure of serious data breaches in the past, demonstrating the inadequacy of the current voluntary notification regime.[viii]

3. Scope

Given the pervasiveness of collection of personal data by organisations of all types and all sizes, and the fact that the size or nature of the entity from which a breach occurs has no effect on the potential for harm, EFA believes that both the Privacy Act itself and a mandatory data breach notification obligation should be extended well beyond the existing scope of the Privacy Act. EFA does however acknowledge that this would involve a potentially significant increase in the regulatory burden for smaller organisations that are not necessarily well-placed to absorb such an additional burden in the short-term. EFA therefore recommends that the scope of the Privacy Act and a mandatory data breach notification obligation should be gradually extended over the medium term.

EFA is concerned that allowing enforcement agencies to self-determine whether a breach should be excepted from the notification requirement is likely to lead to exceptions becoming the default approach.

EFA therefore recommends that the oversight agency should be empowered to make determinations about whether enforcement agencies should receive exceptions, on a case by case basis.

4. Oversight

It is self-evident that the effective operation of a mandatory data breach notification obligation requires an effective, properly-resourced oversight agency.

EFA again calls on the government to ensure that the statutory roles of the Privacy Commissioner, the Australian Information Commissioner and the Freedom of Information Commissioner are filled with long-term appointments and supported by appropriate levels of resourcing.[ix]

5. 'Serious' test

EFA is concerned that the qualification 'serious' associated with both 'risk' and 'breach' in the proposed legislation is undefined and therefore effectively meaningless.

EFA therefore supports the Australian Privacy Foundation's policy that the threshold for requiring notification should be based on either of the following conditions being satisfied:

(a) a real risk of harm without qualifications, such as the proposed "serious" risk; or
(b) a significant breach, whether or not real risk of harm has arisen

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

EFA further agrees with the Australian Privacy Foundation that the default position should be that a breach meets these conditions, unless the entity can establish categorically 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.

6. Notification fatigue

EFA acknowledges that a potential issue with the mandatory data breach notification obligation may arise from 'notification fatigue'. This concern essentially relates to the potential for users to become dismissive of data breach notifications and disregard their importance. It is EFA's view that this is only likely to be an issue in circumstances were a large volume of users are repeatedly notified of a data breach(es).

In this regard, EFA makes two recommendations:

1. Regulatory oversight through the Privacy Commissioner be extended to include a compliance audit process for organisations that are required to send more than **###** notifications in a single calendar year; and/or
2. End-users be provided an option to 'opt-out' of receiving data breach notifications on the condition that such an opt-out option would be only be possible once the end-user has demonstrated that they reasonably understand the consequences of such a choice.

7. Responses to questions posed in 2013 Discussion Paper

The following responses are to the specific questions raised in the 2013 Discussion Paper of the Privacy Amendment (Privacy Alerts) Bill 2013[x], which EFA believes remain pertinent to this consultation.

1. What is likely to be the 'paper burden' or administrative costs (quantified if possible) to private sector organisations under the mandatory scheme in the Exposure Draft Bill? In particular, what will be the burden for entities that:

a. Have existing systems in place to comply to make notifications (where necessary) consistent with the existing voluntary Data Breach Notification Guide of the Office of the Australian Information Commissioner?, and

b. Have no systems in place and may have 'start up' costs?

The additional burden of compliance will be minimal for a mandatory scheme for organisations that have existing systems in place. The burden of compliance for organisations without existing systems will of course be more significant, primarily concerning the establishment of internal procedures and training staff, however the costs involved are likely to be mostly one-off and EFA firmly believes such costs should be considered a normal operational overhead for any organisation handling private data.

In both cases, communication to customers, members or stakeholders is a routine operational practice for which most organisations will have existing systems in place, and the additional expense involved with sending a notification about a data breach should therefore not be significant. To the extent that there is an additional cost involved, this should act as an incentive for organisations to prioritise data security more highly than they may at present.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

2. In your view, will particular industry sectors incur costs disproportionately under the scheme in the Exposure Draft Bill than other regulated entities under the Privacy Act 1988?

EFA does not believe that any particular industry sectors will incur disproportionate costs under the proposed scheme. EFA believes that it is proportionate for entities which conduct business to have satisfactory systems in place to ensure that fundamental rights, such as privacy, are duly acknowledged and safeguarded.

3. Will the scheme in the Exposure Draft Bill result in any restrictions on competition?

Though the impact of any new regulation will be more significant on smaller organisations, EFA believes that data security and compliance with the proposed scheme should be considered as a normal operational cost, in line with other regulations that all organisations must comply with, such as other privacy regulations, workplace safety regulations, etc. EFA therefore does not believe that the proposed scheme will result in any material restrictions on competition.

---

[i] http://www.alrc.gov.au/publications/report-108

[ii] http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/244%20Joint%20Committees/PJCIS/DataRetention2014/FinalReport_27February2015.pdf?la=en

[iii] https://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx

[iv] Serious Invasions of Privacy in the Digital Era (ALRC Report 123), at: http://www.alrc.gov.au//publications/seriousinvasions-privacy-digital-era-alrc-report-123

[v] Standing Committee on Law and Justice, "Remedies for the serious invasion of privacy in New South Wales', available at: http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/0f02a41f813cf811ca257f6a007f7bb2/$FILE/Report%20no.%2057%20Remedies%20for%20the%20serious%20invasion%20of%20privacy%20in%20New%20South%20Wales.pdf

[vi] Law Reform Committee, "Inquiry into Sexting – Final Report", available at: http://www.parliament.vic.gov.au/57th-parliament/lawreform/article/944

[vii] ALRC, Serious Invasions of Privacy in the Digital Era, available at: http://www.alrc.gov.au/publications/serious-invasions-privacy-dp-80

[viii] Draft Early Assessment Regulatory Impact Statement – Privacy Amendment (Notification of Serious Data Breaches Bill) 2015 [DOCX 175KB], page 10.

[ix] https://www.efa.org.au/main/wp-content/uploads/2016/01/OAIC-funding-release-160120.pdf

[x] http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1213a/13bd146

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188