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

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

20th June 2013

Dear Secretary,

Re: Privacy Amendment (Privacy Alerts) Bill 2013

Electronic Frontiers Australia (EFA) appreciates this opportunity to comment on the Privacy Amendment (Privacy Alerts) Bill 2013. EFA has previously provided input to the Attorney-General's Department at earlier stages of the development process for this Bill.

General comments

EFA has been a supporter of the introduction of regulations requiring notification of data breaches involving private data for some time, and therefore strongly supports this legislation in principle. EFA however has some concerns with the bill in its current form, as outlined below.

Applicability

EFA is concerned that as this legislation is only applicable to organisations to which the Australian Privacy Principles apply, its impact on improving privacy protection will therefore be limited, as many of these organisations are likely to already have relatively robust data security measures in place.

EFA understands that the burden on smaller organisations, to which the Australian Privacy Principles do not currently apply, of implementing robust data security measures will be relatively higher. EFA also recognises that the oversight burden on the Office of the Australian Information Commissioner would also increase significantly, if the scope of this legislation were widened to include organisations to which the Australian Privacy Principles do not currently apply. EFA does however believe that widening the applicability of this legislation would be likely to dramatically increase its effectiveness in protecting the private information of Australians.

Minimum data security standards

EFA also recommends that, as suggested by Securus Global[1], minimum data security standards, including monitoring practices, be developed in consultation with relevant industry and civil society organisations. These standards should build on existing best practice standards already available and should be framed to provide practical guidance to organisations of all sizes and across all sectors that collect private information. Education and media campaigns and an outreach program utilising a broad range of representative industry associations should be conducted to maximise the adoption of these standards.

[1] See: http://community.securusglobal.com/2013/05/29/mandatory-data-breach-notification/

Nature of harm

EFA believes that the definition of harm in section 26ZE should be expanded to include:

- psychological harm
- onerousness and inconvenience to the individuals affected
- harm caused by breaches of inaccurate data (which in many cases will cause more serious harm than for breaches of accurate data)

If the definition of harm is not expanded, EFA believes all references to 'serious' should be removed from 'serious data breach'.

Exceptions under section 26ZC

EFA is also concerned about the lack of judicial or parliamentary oversight involved with the exceptions that prevent the Commissioner from directing an entity to provide a notification of a serious data breach, as defined in Section 26ZC, sub-sections 5 and 6.

With regard to sub-section 5 (b), EFA believes it is appropriate that certification of reasonable grounds for an exemption for an enforcement body is required, however this "certification" does not appear to be a sufficiently powerful mechanism for ensuring the accountability of enforcement-related data. EFA is concerned that the simple certification process outlined could too easily become an ineffective 'rubber-stamp' procedure. EFA believes that the Act should specify the full certification process to be followed in these cases, and that there should be some form of judicial or parliamentary oversight of this certification process to ensure that the process is being followed correctly.

With regard to sub-section 6, EFA is similarly concerned that an even lower standard of accountability is being applied to the determination of inconsistency with secrecy provisions than for enforcement-related data. Unlike sub-section 5 (b), sub-section 6 does not even outline a mechanism for making such a determination. EFA believes that, as above per sub-section 5 (b), the process for determination of inconsistency with secrecy provisions should be fully specified, and that judicial or parliamentary oversight should be included.

Judicial or parliamentary oversight is necessary because decisions about data of this sensitivity need to be held to a very high standard of accountability. EFA understands that, in relation to both sub-sections 5 and 6, this oversight may need to be conducted in-camera, with a mechanism described for the application and form of an in-camera hearing. In-camera hearings should still be subject to oversight and the proceedings should still be available upon request for legal purposes such as criminal and civil hearings.

Reporting by OAIC

EFA recommends that the Office of the Australian Information Commissioner be required to compile, report on and publish public notices on a regular (quarterly) basis related to actions it has taken in relation to this Act.

About EFA

Established in January 1994, Electronic Frontiers Australia, Inc. (EFA) is a national, membership-based non-profit organisation representing Internet users concerned with on-line 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 online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Electronic Frontiers
AUSTRALIA

Our major objectives are to protect and promote the privacy and 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's website is at: www.efa.org.au.

Please do not hesitate to contact me if the Committee requires any further information, or wishes a representative of EFA to appear before it.

Yours sincerely,

David Cake
Chair, for and on behalf of the EFA Board