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

Senate Legal and Constitutional Affairs Legislation Committee
Parliament House, Canberra ACT 2600

Via email to: legcon.sen@aph.gov.au

19th December 2016

Re: Privacy Amendment (Re-identification Offence) Bill 2016.

Dear Committee Secretary,

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.

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,

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

Electronic Frontiers
AUSTRALIA

Submission: Privacy Amendment (Re-identification Offence) Bill

Introduction

EFA has been a long-standing supporter of improvements in privacy protections in Australia, and shares widely-held concerns about the threats to personal privacy implicit in the re-identification of publicly-available data sets.

EFA believes the proposed offences will be ineffective in enhancing the privacy of Australians. Further, EFA is seriously concerned that the proposed Bill will criminalise legitimate research activities, such as those dealing with data security and particularly with de-identification and re-identification technologies.

In short, the proposed law is a misguided attempt to deal with a symptom rather than the cause of the issue. As such, the law reveals a concerning lack of understanding of the complexities and challenges intrinsic in data de-identification, and the haste with which it was drafted suggests a knee-jerk response to recent events, rather than a considered, evidence-based approach.

The haste with which this Bill has been rushed into the parliament is in stark contrast to the extraordinarily slow progress the government has made in relation to passage of mandatory data breach legislation. The Attorney-General committed to the Parliamentary Joint Committee on Intelligence and Security to pass such legislation by the end of 2015, however a full year after that deadline, and despite at least two parliamentary inquiries into previous iterations of a mandatory data breach bill, it remains outstanding. Of additional concern is the fact that the current version of the proposed mandatory data breach bill has been significantly weakened by the introduction of significant discretion on the part of affected organisations.

EFA believes that the government should pursue more positive actions to protect the privacy of Australians from data re-identification and other threats by considering a statutory cause of action for serious invasions of privacy at the federal level, as recently called for by the NSW Attorney-General.[i]

Effective de-identification is arguably unachievable

Effective de-identification of data sets is extremely difficult. The Privacy Commissioner has described it as effectively a form of 'rocket science'.[ii]

With more and more aspects of individual's lives involving some aspect of online interaction, and the increasing sophistication of data-mining technologies, the likelihood that even carefully de-identified data sets can be re-identified is also increasing.

It is therefore likely that not even the most expertly de-identified data sets will remain un-re-identifiable indefinitely. This threat is enhanced when considering that re-identified datasets cannot be de-identified once re-identified in the public domain. This irreversible risk of 'letting the genie out of the bottle' should be a primary consideration of policymakers when approaching this topic. EFA warns that insufficient, misguided or ineffective policy at this point may have a catastrophic impact on any future efforts to curb or mitigate the re-identification of sensitive datasets.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

Electronic Frontiers AUSTRALIA

Rather than the *a posteriori* approach inherent in this proposed Bill of imposing sanctions on acts of re-identification after they have occurred, EFA believes the preferred policy approach should be one of attempting to minimise the risk of re-identification.

EFA therefore believes that Australia should adopt an approach encompassing the concept of 'data austerity' (*datensparsemkeit*[iii]), which involves only storing as much personal information as is absolutely required for the business or applicable laws.

Such an approach will likely be a much more effective means to address the risks to the privacy of Australians than this proposed Bill.

No effective deterrent value

EFA does not believe that the sanctions included in his proposed Bill will be effective in preventing re-identification of data sets.

Malicious actors will of course not advertise the fact that they have been successful in re-identifying a data set, except, perhaps in order to sell that re-identified data set to other malicious actors. Otherwise, they will presumably use the data for their own purposes.

Given that using such re-identified data by malicious actors is likely to involve acts that would be subject to existing criminal sanctions, the sanctions included in this proposed Bill are, arguably, redundant.

Many of these malicious actors will of course be based outside Australia, and/or will likely go to significant lengths to obfuscate their location and identity, and are therefore not likely to be deterred by the potential sanctions included in the proposed Bill.

Chilling effect on legitimate Australian research

EFA is concerned that the proposed Bill will inhibit legitimate Australian-based research into data security.

The concept of a 'whitelist' of researchers approved by the Attorney-General is likely to be unworkable in practice and also represents an intolerable intrusion of government fiat into academic research.

The proposed Bill is therefore likely to have a demonstrable effect on the ability of some Australian-based data security researchers to continue their work in this country.

No incentive to improve data security

As noted above, the proposed Bill creates no incentives for Australian government agencies or other organisations to increase their data security, or to adopt data austerity measures.

Conversely, the proposed Bill creates (as intended) a strong disincentive for researchers to announce a real or potential vulnerability of re-identification.

Both of the above will be to the detriment of the privacy of Australians.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188

Electronic Frontiers AUSTRALIA

No redress for affected individuals

EFA is particularly concerned that the proposed Bill provides no form of protection, let alone information or remedy to the individuals affected.

As noted above, EFA believes that the parliament should prioritise a statutory cause of action for serious invasions of privacy (a privacy tort) as an important element in providing individuals with a potential avenue for redress should their privacy be compromised as the result of the re-identification of a data set.

Clearly, in order to be effective, such a cause of action should not include an exemption for government agencies, where it can be proven that inadequate steps were taken during the process of de-identification.

Recommendations

1. **the proposed Bill is fundamentally misguided and should not be passed in any form**
2. **the Parliament should work towards the introducing of data austerity (minimisation) rules into the Australian Privacy Act and into Australian Public Service guidelines**
3. **the Parliament should introduce a statutory cause of action (privacy tort) for serious invasions of privacy**
4. **the parliament should pass the proposed mandatory data breach notification bill, but should reject the recently-introduced changes that introduce significant discretion for affected organisations.**

Acknowledgement

EFA gratefully acknowledges the support of the Australian Privacy Foundation in drafting this submission.

[i] See: http://www.smh.com.au/nsw/only-one-piece-of-the-puzzle-baird-government-calls-for-national-privacy-laws-20161207-gt6ibl
[ii] See: http://blog.cebit.com.au/deidentification-privacys-rocket-science
[iii] See: https://www.thoughtworks.com/radar/techniques/datensparsamkeit

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188