AUSTRALIAN BANKERS' ASSOCIATION INC.
Strong banks – strong Australia

Level 3, 56 Pitt Street
Sydney NSW 2000
Australia
+61 3 9852 7976
@austbankers
bankers.asn.au

21 December 2016

Ms Toni Matulick
Committee Secretary
Senate Legal and Constitutional Affairs Legislation Committee
Parliament House
Canberra ACT 2600

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

Dear Ms Matulick,

# Privacy Amendment (Re-Identification Offence) Bill 2016

The Australian Bankers' Association (ABA) appreciates the opportunity to provide its comments for the Committee's consideration for its inquiry into the Privacy Amendment (Re-Identification Offence) Bill 2016 (Bill).

With the active participation of 25 member banks in Australia, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

To begin, we note that the Productivity Commission's Inquiry into Data Availability and Use (PC Inquiry) is simultaneously proposing a new framework for data sharing, including public sector datasets and those that comprise identifiable data. In addition to deterrence measures such as the re-identification offences regime in the Bill, it is equally important that the public sector follows high standards for publication of de-identified data, including appropriate controls, protection and de identification practices before publishing data.

We believe that this preventative framework needs to be developed in tandem with deterrence measures such as the re-identification offences regime in the Bill.

## 1. Introducing criminal offences into the Privacy Act

The ABA is concerned that by a single issue amendment to the Privacy Act, criminal offences are to be introduced into the Australian privacy regime under which the long standing, accepted sanctions for an interference with an individual's privacy are civil penalties. This is proposed without a full and proper consideration of the whole of the Act.

If this is to be the Government's intended approach to the Act, this should be the subject of a more formal and detailed review of the Act, not simply because of one ad hoc amendment to the Act.

This concern is elevated because of the intended retrospective application of the Bill, its commencement on the day after the Bill receives the Royal Assent and the very substantial number of resources and systems changes that may be necessary to be undertaken by our members to ensure compliance with the broad requirements of the Bill.

Further detail about these matters follow in this submission.

Strong banks – strong Australia

## 2. Impact on innovative, beneficial data use

The ABA and its members recognise that the need to protect the rights of individuals[1] must be carefully balanced against the benefits that innovative uses of data can provide[2], including benefits to the community at large and consumers individually. We suggest that while the Bill goes to the former aim, it does not adequately consider the latter aim because of uncertainty that will be created for businesses seeking to use public sector data.

Quoting from the PC Inquiry draft report: "*increased access to data can facilitate the development of ground-breaking new products and services that fundamentally transform everyday life… but better access to and use of data can also benefit business and government through improved operational processes and productivity.*" This is certainly the case in the financial services sector.

The ABA and its members consider that the proposed regime set up by the Bill creates significant uncertainty for businesses which might otherwise use public sector data for legitimate commercial applications that create broad-ranging benefits. These new risks may mean that businesses choose not to use public sector de-identified data at all, reducing the benefits that could be realised from its use.

While very few current activities by industry could be expected to be captured by the proposed rule, as the PC Inquiry draft report recognises, "*opportunities to use [data] are largely unknown until the data sources themselves are better known, and until data users have been able to undertake discovery of data.*" That is, while it is yet unclear what kind of community and economy-enhancing uses might be made of data as its availability and uses increase and with improvements in data analysis techniques, we believe this will increase exponentially.

Some of this uncertainty might be resolved by giving consideration to requiring that the public sector publisher of de-identified data articulate the rights (and purposes) for which the data is being made available.

The proposed regime also does not appear to consider what happens to the broader use of an existing de-identified Government data set, in circumstances where it has been re-identified by a specific third party. Would all users thereafter be prohibited from using that data set, whether or not these users themselves engage in any re-identification activities? Such a ban would have major implications for data analytics, particularly as after multiple steps of data processing it can be a challenge to ascertain where a de-identified Government data set was used (at some point in the chain of data processing and analytics).

One issue will be how simple it is to determine whether a Government data set is published by an agency 'on the basis that it was de-identified' personal information. The Explanatory Memorandum notes that what is relevant here is the intention of the agency, and not whether it was possible to re-identify the information. For organisations operating within the proposed regime, subjective intention would be a challenge to interpret, creating additional uncertainty about the use of public sector data more broadly.

## 3. Retrospective criminal offences and civil penalties for re-identification conduct from 29 September 2016

The substantive enactment commences on the day after its Royal Assent.

For banks and other large businesses the timeframe for implementation of systems and personnel controls to prevent intentional (and unintentional, accidental) re-identification of published de-identified Commonwealth agency data is short and to discover data that has been re-identified back to 29 September 2016 (and before then) and to notify the responsible agency is too high a duty.

Even with prospective application of this regime, for banks and other large businesses, significant time and resources will need to be invested in building new governance processes and systems specifically

[1] The Privacy Amendment (Notifiable Data Breaches) Bill 2016 will address one of these aspects.
[2] The ABA acknowledges the steps being taken towards this by the current Productivity Commission inquiry into Data Availability and Use.

Strong banks – strong Australia

dealing with de-identified Government data sets and the re-identification regime (including testing awareness, intention etc), to ensure compliance by the organisation and staff.

The reference in the Bill to Criminal Code sections 11.1 (attempt), 11.2 (aid, abet, counsel or procure), 11.4 (incite) and 11.5 (conspire) will apply to clause 16D(6) (and to clause16E(7)) offences shows the significant scope of developing governance processes and systems.

Under the Bill, an offence applies to an "entity" which includes an "organisation" which in turn includes an individual or a body corporate.

The Criminal Code includes knowledge, recklessness and negligence as part of any fault element.

Given the retrospective application of the Bill's regime and the significant task ahead for our members to ensure they have robust compliance systems and processes in place to avoid a breach of the regime, a defence should be considered for inclusion in the Bill. Such a defence would entail that the entity had acted reasonably, in good faith and in the circumstances ought fairly to be excused.

## 4. Clause.16D -Intentional conduct (criminal and civil penalty)

There are foreseeable situations where a large organisation that engages in data analytics might breach this provision, for what might be considered a 'legitimate' purpose.

An example is where a de-identified Government data set is used, and at some stage in the analytics process is combined with another data set, for commercial purposes including better consumer choice, and this leads to re-identification of the information.

It is unclear in this situation whether the 'intention' requirement would be satisfied and thereby constitute a breach of the provision (e.g. because the data analyst working for the organisation knew there was a possibility this might be the outcome), or whether it would only be captured under proposed section 16F.

Perhaps the uncertainty introduced by the 'intention' element could be mitigated by it being a higher threshold e.g. where the dominant intention was to achieve the result that the information is no longer de-identified.

It will be crucial to define what re-identification means, and guidelines may be useful to help organisations ensure they have sufficient safeguards to ensure compliance (and to ensure an organisation is aware when re-identification does occur). Under the Privacy Act "de-identified" personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

Through analysing de-identified data, or by appending an organisation's data to a small number of records, it may be possible to re-identify data in a (statistical) estimate sense.

Clarity is necessary on this and consideration could be given to the guidelines the Australian Bureau of Statistics has in place around releasing confidential datasets from the census.

## 5. Clause16E- Conduct resulting in re-identification and disclosure(criminal and civil penalty)

This offence requires no intention other than for the entity to disclose the information to a third party which the entity has caused to be de-identified and is aware this is the case.

This emphasises the need for internal compliance systems that are able to ascertain this and to manage the risk.

Banks are required to report very large amounts of data to Commonwealth Government agencies.

A question is what would be the implications for reporting of data by banks to these agencies such as the Reserve Bank of Australia (and for that matter any data reported to a Commonwealth agency) and

Strong banks – strong Australia

these data become Commonwealth agency data. Under the Bill where the data is de-identified in an agency's hands these data may still be identifiable data in the bank's hands.

Arguably, the bank has not taken an act to re-identify the data because it is its own data. However, are there likely to be consequences for the bank because it had failed to de-identify these data (an omission to act) or disclose these data to a third person?

It will be critical for this uncertainty to be resolved in favour of the bank by the Bill.

## 6. Clause 16F Notification of responsible agency (civil penalty)

An entity would have to be able to ascertain that it knows re-identification has occurred (intentionally or innocently/accidentally). A question is whether it is practicable for the entity to notify the responsible agency as soon as practicable after becoming aware (clause16F(3)) and not to use or disclose it to anyone else (clause16F(4))?

Large organisations including banks could engage in behaviour that would fall under proposed section16F. For example, a bank may use a de-identified Government data set to verify the bank's own information.

In this situation, re-identification of the Government data set might accidentally occur, without the bank intending for this to happen.

As submitted above, the Bill should provide a defence for such outcomes where the bank acted reasonably and in good faith and in the circumstances ought fairly to be excused.

## 7. Clause 21 Transitional – notification of identification occurring prior to commencement

The Bill and the Explanatory Memorandum (EM) should take into account under proposed sections 21(2) and 21(3) that the notification to the responsible agency as soon as practicable after the entity becoming aware that re-identification of relevant de-identified information has occurred, or that this information has been used or disclosed to a third person, that the Bill will commence on the day after the Royal Assent, that its application is retrospective and that entities will need time and extensive resources to put their compliance arrangements in order.

## 8. Clause16G - Exempt entities

The EM notes that the exemption in clause16G is expected predominantly to protect entities 'engaging in valuable research in areas such as testing the effectiveness of de-identification techniques, cryptology or information security', though a public interest determination power is available in the event a different legitimate purpose arises in the future.

We would appreciate clarity on whether commercial organisations conducting such activities might be entitled to the Minster's determination that banks engaged in these data activities should be exempt either on public interest grounds or for the (non-exclusive) purposes referred to in clauses 16G(2)(a)-(d).

Further, we query whether the types of activities envisaged by clause 16G are framed too narrowly. As noted above, there is wide recognition that commercial use of data can result in benefits being realised for the community more broadly and consumers in particular, in addition to achieving economic efficiencies and innovation.

Regardless of how wide the range of activities envisaged under clause16G are, it appears that a less resource-intensive administrative approach would be to have these operate as a 'defence' to an allegation, rather than requiring the Minister to make a determination for each potential entity (or class of entity) that seeks to apply for an exemption.

Strong banks – strong Australia

Otherwise, as the Bill will commence on the day after the Royal Assent, consideration should be given to enabling applications for exemption determinations to the Minister before commencement with effect on commencement.

## 9. Concluding comment

According to a media report[3] the "trigger for the sudden announcement [by the Attorney-General] is understood to have been a data breach at the Department of Health that was revealed today [29 September 2016], which saw anonymised doctor ID numbers decrypted by academics testing the quality of the department's encryption methods."

The ABA acknowledges the seriousness of this privacy breach possibly due to alleged deficiencies in the encryption methods involved. The imposition of criminal offences across the broad spectrum of private sector organisations arising from this single instance where it is not evident that serious or any harm resulted for the individuals concerned, and without detailed analysis and consideration of the potential impacts on and implications for legitimate security and data analysis activities, should be considered carefully. In particular, any proposed criminal offence should be balanced against the effectiveness of existing civil sanctions that exist under the Privacy Act and the more serious implications for the private sector.

Yours sincerely

Ian Gilbert
Director Banking Services Regulation
igilbert@bankers.asn.au

[3] http://www.itnews.com.au/news/brandis-says-white-hats-will-be-exempt-from-data-law-changes-438496