Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

27 September 2016

Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

By email: economics.sen@aph.gov.au

Inquiry: Census 2016

This submission from the Australian Privacy Foundation (APF) responds to the Senate Inquiry into the preparation, administration and management of the 2016 Census by the Australian Bureau of Statistics.

It largely covers the issues around privacy arising from the new uses of name and a unique identifier (SLK), and lack of transparency on the part of ABS about the implications of these changes. It touches on the breach of trust that has occurred from this change, the apparent change of the Census from statistics to surveillance, suggestions for legislative protection from these changes, the significance of control of personal information as the basis for trust, the privacy implications of the unique identifier and a variety of other issues. A major theme is the lack of transparency being shown from an entity that is insisting, under threat of prosecution, that Australians be highly transparent to it.

This submission does not deal at length with the abandonment of the web site at around 8 pm without notification, leaving millions dutifully “coming back in 15 minutes” as instructed after a series of technical failures apparently culminated in wrongly attributing internal log and system info going to a US IBM operations centre as ‘exfiltration’ of census data. Others will not doubt focus on those more obvious indications of a failure to address information security risks.

Contents

General comments 3
Terms of Reference 5
a) The preparation, administration and management on the part of the Australian Bureau of Statistics (ABS) and the Government in the lead up to the 2016 Census 5
b) The scope, collection, retention, security and use of data obtained in the 2016 Census 9
c) Arrangements, including contractual arrangements, in respect of the information technology aspects of the Census 11
d) The shutting down of the Census website on the evening of 9 August 2016, the factors leading to that shutdown and the reasons given, and the support provided by Government agencies, including the Australian Signals Directorate. 12
e) The response rate of the Census and factors that may have affected the response rate 12
f) Privacy concerns in respect of the 2016 Census, including the use of data linking, information security and statistical linkage keys. 12
g) Australia's Census of Population and Housing generally, including purpose, scope, regularity and cost and benefits 14
h) The adequacy of funding and resources to the ABS 14
i) Ministerial oversight and responsibility 14

General comments

Breach of trust

Before the 2016 Census, the Australian public (generally) trusted the ABS. This is no longer true for a significant part of the population.

The trust was not destroyed because the ABS and its contractor IBM were incapable of running an online census on census night 2016. (Though of course the multiple technical, planning, risk mitigation, managerial, communication and IT security failures -- on display to the millions of Australians who wasted millions of hours taking the repeated request “come back in 15 minutes” on face value when the back end of the site had been suspended and abandoned by its panicked operators -- certainly reveal no basis for trust in data governance and digital systems competence of ABS or government.)

Instead, the basis for that trust was destroyed when the ABS decided to change the purpose of the Census from aggregated statistical data to personal tracking: a change from statistics to surveillance.

The APF supports the original purpose of the census, being to collect aggregated statistical data for the purpose of public planning. For a century the effectively anonymous snapshot model served this purpose well, and built the precious reserve of public trust which is now being squandered by ‘disruptive innovators’ willing to burn it to make this change.

Restoring trust by embedding protections in the Act

That original, trustworthy purpose can be confirmed by amending the legislation along the lines set out below to protect the safe and accepted approach from this change.

Recommendations for legislative change:

1. Provision of name, and other key identifiers, is not compulsory.
   Amend Clause 7 of the Census and Statistics (Census) Regulation 2015 and its successors to remove the following from the prescribed set of ‘statistical information’:

   a. Name (item 1)*
   b. Sex to include intersex (item 2)*
   c. Full Date of birth (item 3)*, but with Age in years to remain
   d. Name and address of employer (item 20(c)).
      [* the three elements typically transcribed into an SLK identifier or any unique identifier]

2. Key identifying data is not collected or used for longitudinal or external data linking.
   Amend the Census and *Statistics Act 1905* (CSA) to prohibit:

   a. the collection or use of Name,
   b. the use and retention of full Address other than for administering the census collection itself, and
   c. data-linking of Census data on a unit record level; whether between successive censuses or across other externally-sourced datasets; and whether using name, address, date of birth, sex, other identifying data fields, SLKs, probabilistic linking or any other identifying method.

3. If Name is provided, it is destroyed within a short period, and not retained for other than short term administration of a given Census.
   Amend the CSA to this effect.

4. Data breach reporting is mandatory, with notification of individuals and regulators. Amend CSA to require a notification of a breach (including re-identification) of data collected by a Census, wherever and by whomever the data was held when breached. Pass comprehensive mandatory data breach notification laws, creating enforceable rights for individuals, like those tabled in 2013 or promised in 2015 to secure telco data retention.

If the above measures were taken now, it is possible that trust could be restored to the ABS.

Privacy as the control of personal information

The Privacy Commissioner, Timothy Pilgrim has said in a recent speech:

"Privacy is not secrecy. It is about giving individuals control over how their personal information is handled; giving customers confidence and trust."

The APF contends that this concept, which has been restated by numerous scholars, courts and officials since the 1970s, is the key issue at the heart of the failure of the 2016 Census. Many Australians no longer have confidence and trust in the ABS and its future plans for the use of their data.

The ABS has continually asserted that it is completely committed to secrecy, and draws attention to penalties. This appears to be a deliberately misleading attempt to encourage Australians to overlook the main issue, which is *how the data will be used*. Many Australians are no longer persuaded by this attempt at misdirection, and it shows in the public concern and outrage in relation to the 2016 Census.

If the Australian Government is committed to privacy, and in particular giving Australians reasonable control over how their personal information is used, it must reject all of the ABS's move from statistics to surveillance, and in particular its plans to turn every Australian into a unique digital identifier (SLK).

We draw attention to APF's outline of Meta-Principles for Privacy Protection, at http://www.privacy.org.au/Papers/PS-MetaP.html

There must be no "Australia Card for Big Data" by digital stealth

The government is increasingly using a unique identifier (a Statistical Linkage Key) for individuals using government services. Both health and social services use this key, or a variant of it, for identification of unit level records. The ABS is using an apparently compatible SLK for similar purposes (in the absence of an effective PIA and with ABS unwilling to discuss identification issues in any depth, it is difficult for outsiders to confirm the actual algorithm used).

An SLK is supposed to be 'anonymous' and we understand the most commonly used version is a combination of parts of the last name, part of the firsts name, date of birth in the clear, and a number for sex (1 or 2) in the clear.

While the extraction of letters from a name may offer a form of weak obfuscation from casual inspection (the name is not spelled out in full, so you couldn't quickly tell the name of a patient file with an SLK on the cover), and reconstruction of the full name from scratch with no other aid is impeded, it offers no meaningful identity protection from any serious use. Anyone can derive an SLK for any person once you have their name, DOB (which can be discovered in various ways), sex (which is generally obvious) and algorithm (which is well known); you could easily match the person with their SLK from a small list; and given sufficient access to other data sets (whether proprietary, public or accessible by government) and Big Data tools, you may be able to identify records on a large scale.

We contend that:

(1) an SLK is an identifier
(2) the privacy protection that an SLK provides is negligible
(3) data carrying an SLK is emphatically **not** de-identified or anonymous
(4) the SLK, quite simply, is, and appears designed to be, a de facto national identifier
(5) the public will quickly come to understand that to be the case, and
(6) this may result in the collapse of public confidence in government and widespread reduction in the preparedness of the public to provide accurate data to government agencies

In the past Australians comprehensively rejected the introduction of an Australia Card. The ABS is using and promoting the SLK, and has the most comprehensive store of data on Australians. The extended use of the SLK is in fact a form of digital "Australia Card", and one which has new dangers in the context of 'Big Data'. This type of tracking must be comprehensively rejected as it is not relevant to the objectives and purpose of the census.

(We discuss below the failed internal Privacy Impact Assessment by the ABS in 2015, which, in contrast to the exercise which largely rejected the similar name-identified-record proposal in 2006 as too intrusive, did not engage with stakeholders or give an opportunity for considered analysis of the details. Because of ABS's choice to avoid effective notification of that PIA exercise in 2015, and their later unwillingness to provide answers to our written and in person questions on identification risks and identifiers, we and other outsiders are therefore working at a disadvantage in not having access to full information about the SLK as ABS proposes to construct and use it. However the outline of the proposed expansion of data linkage by SLK seems clear.)

Terms of Reference

a) The preparation, administration and management on the part of the Australian Bureau of Statistics (ABS) and the Government in the lead up to the 2016 Census

The consultation process by the ABS in relation to proposed changes to the Census was at best incompetent and at worst a sneaky attempt to make serious changes without anyone noticing. The APF was not specifically consulted about the proposed changes and we were completely unaware of the consultation, as it seems were other interested NGOs. The ABS did not contact us in any way about the consultation. It is noted that an internet search on privacy advocacy groups reveals the APF as the top listing. In any case, the APF is hardly unknown to the ABS. The APF led the campaign against the ABS' proposal to retain names in 2006, with considerable success. By any measure, the consultation process was completely inadequate given the serious change proposed.

If the purpose of the ABS was to avoid a campaign to oppose the census changes, it was partially effective in slowing down sounding the alarm and organisation of a campaign. In the end, we and other concerned parties only had a few months to advocate against the changes. Of even more concern, many Australians never got a complete understanding about the meaning and impact of the changes. The campaign is ongoing as the problem is not resolved.

Also of concern are recent statements to the effect that the Census is now 'a success', because it is clear from our experience that Australians did not have before them adequate information on which to assess the safety or otherwise of the new surveillance model of the census, or ABS' precautions in relation to de-identification of the newly identified lifelong data dossiers to be kept on each Australian. Trust and compliance based on ignorance and obfuscation is not sustainable.

When APF found out about the missed consultation process and the proposed changes to the census we immediately wrote to David Kalisch, Australian Statistician on 12/02/16.[1] The letter raised concerns about the Privacy Impact Assessment and the consultation process,

[1] A copy of the letter can be found at https://www.privacy.org.au/Papers/ABS-CensusPIA-160212.pdf.

Following the APF's letter to Mr. Kalisch, the ABS arranged a meeting with the APF on 14/3/16. Mr. Kalisch did not consider it necessary to attend the meeting. At that meeting with the ABS the following matters were discussed:

1. They had not heard of the APF and that is why we were not consulted. The APF found this hard to believe and said so. (Their previous PIA provider was well known as an APF policy director)
2. We asked why an external PIA was not done. This question was not answered.
3. ABS assured us that it took its secrecy provisions seriously. The APF made it clear our concerns were about the use of data, and also noted that IT security is now always at risk, with data as the new 'Toxic asset' described by security expert Bruce Schneier, and the best protection of sensitive personal information is not to collect it, or at minimum destroy it straight away.
4. ABS told us that the Federal Privacy Commissioner and State privacy commissioners had all been consulted on the plans and did not express any concerns. We observed the lack of jurisdiction or power of the state entities, that the Federal regulator was at the time in a part-time, temporary appointment in an agency paralysed by its attempted abolition, and that their apparently unconcerned participation in a PIA that did not consult or engage with the 25 million people affected was a matter of concern rather than a comfort (see below).
5. The APF made it clear we were not satisfied with their verbal responses, since they did not engage substantially with either the public engagement or information security threat questions we had asked, and we wanted a written response to our letter.

A written response was received on 31/3/16 from the ABS[2]. The letter does significantly say:

> "I would like to specifically confirm that the ABS is not willing to, or legally permitted to, publically [sic] release data in a manner that is likely to enable the identification of a person or household. The ABS never has and never will make identifiable Census data or microdata publically [sic] available through our statistical or microdata releases. Re-identification protections are inherent in this commitment."

Our concerns about personal information security, expressed in our original letter and in the meeting and seemed not to have been grasped by ABS, given these generic assurances were a repeat of statements on their web site. Our concerns were that:

a) the proposed uses of the name and the SLK derived from it by linkage, data matching or other virtual connections with re-identifiable unit records within government (and perhaps with other outside entities and agencies such as researchers), and longitudinally within the ABS, were a dramatic and fundamental change from the safe anonymous snapshot model assumed and trusted by Australians, and were a privacy-intrusive re-use for a different purpose and with different risks to the trusted original model -- which by inherent design did not expose individuals to the risk of re-identification and later inappropriate use.

   (this is not about *publicly released* data, it is about the use of data by ABS and other bodies, and their facilitation of data linkages and long term identification through SLK); and

b) when apparently de-identified data is made public, the dangers of re-identification arising from the proliferation of Big Data tools and data sets released 'into the wild' have grown dramatically in the last few years. Our concern, based on indications of loss of expertise at ABS during the recent repeated cuts and lack of experts robustly engaged in pursuing this emerging threat in other federal agencies, was not that ABS would wittingly enable re-identification, but that it did not appear to appreciate that the danger was from external entities taking matters into their own hands and bypassing protections by using re-identification techniques and data sources that were unviable or unavailable even a few years ago.

[2] Available at https://www.privacy.org.au/Papers/ABS-CensusPIA-Reply-160331.pdf

> In the light of recent work like that of NICTA researchers proposing that privacy protection from data obfuscation loses effectiveness every year,[3] even with current technological methods, we were interested in how far into the future ABS had projected the degradation of the effectiveness of its existing de-identification methods, because once a collection is released into the wild, there would be no capacity to call it back if there was a subsequent breach.

The APF found the ABS to be dismissive of our concerns, which still have not been substantively addressed. ABS continues not to be transparent how the data will be used, how the linkage keys will be used and interact with the huge array of data where unit records are identified by SLKs, and how retention of identifiers like name and data of birth and their transcription into a permanent lifelong SLK is justified in light of the risks.

The failed 2015 Privacy Impact Assessment

A Privacy Impact Assessment (PIA), properly and independently conducted, is a well-established should be an essential and rigorous tool for discovering and understanding the full range of information security, data protection and privacy risks in a proposal; for enabling well-informed community, expert and stakeholder input to aid that process; and for supporting transparency and evidence-based analysis of the adequacy of proposed remedies for those risks.

We refer to the *Guide to undertaking a Privacy Impact Assessment* from the Office of the Australian Information Commissioner (OAIC), at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.This confirms that the purpose of a PIA is to identify possible impacts on the privacy of individuals and develop "recommendations for managing, minimising or eliminating that impact."

It also observes that if a PIA is not conducted properly, it can have a significant impact on the community's trust in the entity.

We contend that the internal PIA conducted by the ABS in November 2015 and released just prior to Christmas did not meet the above *Guide* standards, and the resulting lack of trust when people started to understand what was proposed was entirely predictable given the poor PIA. It is hard to think of an example of a PIA that would be more important than the PIA for a census, especially one that proposed to drop the inherently safe name-agnostic approach proven over a century for a radical change to use a longitudinal and potentially cross agency identifier. Yet despite how important the PIA was, the ABS chose to do an internal PIA, one which conveniently could not see any real issues and found that they could do exactly what they proposed to do with a "very low" risk of any problems. As history shows, the risk was not very low. This shows the PIA to be quite unrealistic and suggests it was in effect set up to be just a rubber stamp exercise.

This represents a serious governance failure. It is using a PIA to undermine instead of protect privacy. By accident or design it failed to properly identify either the privacy risks or the reputation risks from the proposal itself, and clearly also failed to identify the IT security and infrastructure provisioning risk of the other proposal to push the majority of responses online on a cut price system procured without a tender when there was no-one at the helm.

We can only assume that the ABS apparently hoped that no-one would notice or care about any of the privacy issues that had caused the plan to be set aside in 2006, and not pursued in 2011, and that they could talk their way out of it relying on the century of trust accrued by the old safe model. And that they could outsource their responsibility for IT in this post-IT-security world.

Of further concern, is the apparent failure of the role that the Privacy Commissioner should have played in relation to the proposal, and to the 2015 PIA, in particular.

[3] M. A. Rizoiu at al, 'Evolution of Privacy Loss in Wikipedia,' WSDM'16, February 22–25, 2016, San Francisco, via NICTA, <https://www.nicta.com.au/pub-download/full/8940/>. See also recent critiques of 'differential privacy' by Arvand Narayan from Princeton, among others. Further references available on request.

We submit that the Committee needs to investigate the exact nature of ABS consultation with the Office of the Australian Information Commissioner (OAIC) and explore why it either failed to adequately raise entirely predictable concerns already identified in the 2005 PIA (and which resulted in the abandonment at that time, of the proposal at it affected 95% of the population), or failed to respond to any concerns raised.

In view of the warning from 2005 that the core proposal was both excessively intrusive and controversial, the Committee should in our view also seek answers from the OAIC why it did not insist on adequate notification of the public[4] nor participation by community, consumer, NGO or advocacy groups able to raise the interests of the tens of millions of people to be affected. As far as APF can ascertain, no other body representing actual data subjects was informed.

(We understand for instance that the RSL were surprised and concerned to find out many months later about the proposal, and would have wanted the chance to raise the interests of service people at risk of operational identification, or of personnel more generally at risk of career compromise through exposure of medical data.) .

The 2015 PIA failed to deal with any of the recommendations made in the independent 2005 PIA, which raised major concerns and was instrumental in leading to the substantial withdrawal of the full name retention proposal for the 2006 Census. The issues in play remained substantially the same with the ABS pushing to keep names and addresses and use this information for more detailed data-matching. The Committee should review the 2005 PIA closely, as it shows the sort of real inquiry which the ABS thwarted by having an internal Clayton's PIA in 2015.

Not one of the recommendations made in the 2005 PIA have been implemented.

In fact, the 2015 PIA failed to adequately address any of the main privacy concerns in any meaningful way.

The ABS thus failed the Australian public when it decided to do an illusory PIA.

Worse still, the 2015 PIA does not even address the concerns about the use of a unique identifier or SLK which is at high risk of re-identification. It does not address data-matching with the unique identifier. It does not even identify the nature of the SLK or the proposed data linkage and matching as a risk. The ABS has talked about "anonymous linkage keys" in the 2015 PIA (only 3 times in the entire PIA) and yet there is no actual analysis of the asserted anonymity or the proposed use of the identifier.

It is impossible for a PIA to meet the standards in the OAIC PIA Guide without addressing all of the serious privacy risks.

In our view the ABS has repeatedly misled the Australian public about the 'anonymous linkage keys'. Ordinary Australians would envisage an 'anonymous linkage key' to be an encrypted key of random letters and numbers that would meet the highest encryption standards and could not be data matched. Instead, the SLK is apparently a non-encrypted key that includes parts of actual personal information in the clear. It is not anonymous. In many contexts it would not be even pseudonymous. It is at real risk of re-identification and there is an intention by the Government to use a standard as an identifier for many purposes, apparently without having reviewed its safety in the new, post-IT-security world of Big Data and massive breaches.

A system needs to be in place to ensure that any PIA meets the required standards. In the case of the 2016 census the PIA process comprehensively failed. A proper PIA is still needed to unravel the implications, risks, and effectiveness of precautions proposed.

[4] The utterly inadequate token media release was so ineffective at drawing attention to itself that it only made it into one public service newsletter and an online media release archiving site -- no real media and no real coverage.

Recommendation 1
That the ABS be required to delete all names and other direct identifiers such as SLKs from personal data that it gathers

Recommendation 2
That the ABS be required to commission a PIA for any proposed changes to the census that may impact the privacy of individuals. The PIA must comply with the OAIC PIA Guide and be conducted by an independent external consultant with extensive privacy experience, and engage adequately with interested stakeholders able to assist its inquiries.

Lack of legislative change is a problem, and makes the Census legally dubious

The current Act that applies is the *Census and Statistics Act 1905*. It is impossible to argue that issues with identity and personal information have not changed significantly since 1905. The Act is seriously out of date and needs to be updated to take into account comprehensive changes in how data is managed and privacy.

Significantly, the proposed changes to the Census in 2016 did not appear to require any legislative change consultation process. The ABS instead did an internal PIA with a very limited consultation process as the only steps needed to make a momentous change to the purpose of the Census. We contend that the ABS has failed to interpret the law properly in relation to the meaning of "statistics" and cannot *require* any Australian to provide their name, as it continues to assert. This is discussed in further detail below. In any event, the significant changes to the Census are a failure of procedural fairness.

Recommendation 3
That the Census and Statistics Act be amended to preclude the ABS from gathering, retaining, and disclosing identifiable personal data.

b) The scope, collection, retention, security and use of data obtained in the 2016 Census

Scope/ 'Scope Creep'

The Census was a relatively stable enterprise for the first century of its operation, and public trust was in part based on the perception that its scope was well understood and acceptable. The ABS has pushed for the scope of the Census to change over the past 10 years, and particularly in the last five. Most Australians understand the purpose of the census to be to collect and publish statistical data for planning purposes. That scope has now been widened to include three key changes (that have happened recently):

1. Compulsorily require unique personal information such as name;
2. Develop a unique identifier (SLK or other type) for every Australian; and
3. Share or enable access to the data attached to that unique identifier with other parts of government for the purposes of data-matching, linkage or other unit-record-level

This 'scope creep' is one of the many, serious concerns about the ABS' recent initiatives. (Scope creep is recognised as a key contributor to IT project and data system failure, and creates governance and risk uncertainty.) The ABS states that the name and address information is needed to provide a "richer and more dynamic statistical picture of Australia." We contend that this means that the ABS wants to retain far more granular statistics that are associated with unique and identifiable individuals. The Bureau itself hinted at this in a 2015 internal paper which set out as an objective: '… to build a reputation as Australia's 'premier integrator of government data'.

The recent scope creep is a major concern given that prior to the changes the ABS had built up decades of trust by collecting statistics for the greater good. That has now changed and it remains unclear how far the data-matching scope actually extends, either already or in future plans.

Recommendation 4
That the Act be amended to ensure that the use of personal data arising from ABS activities is specifically limited to the generation of statistical data, and that scope creep involving the deliberate use of data at the level of identifiable individuals is precluded by law.

Collection

The collection of the Census data has led to widespread reports of harassment and threats to ordinary Australians by Census agents. Many people have concerns about the Census. Those concerns have not been addressed. Despite this, people are being threatened and coerced. It is noted that this type of behaviour is prohibited from Debt Collectors in Australia[5] and yet apparently appears to be encouraged by the ABS.

Some examples of harassment and coercion reported are:

- Being issued with a final notice on 9/9/16 (which states the census is overdue) to complete the census, when it is widely reported that the final date to complete the census is 23/9/16. The ABS website still states as at 21/9/16 that there is time to complete your census.[6] A final notice is misleading. A copy of a final notice received by an individual is attached.
- Residents being told that the due date was the 14/9/16 which is clearly not correct.
- Residents who are very unwell being repeatedly badgered by census agents. There does not appear to be any process in place for extenuating circumstances.
- Census agents telling residents that fines will apply every day from 9/9/16 (again in contradiction with the ABS website).

The harassment has been unprecedented. It is unclear how the ABS proposed to build trust with the public by threatening them. What the ABS fails to understand is that Australians completed the Census over many decades because they understood the public good. The remote prospect of fines was never a significant contributor to that decision. Punitive and potentially unlimited fines should not be used, either now or in future.

Recommendation 5
That the ABS be prohibited from misleading, threatening, harassing and coercing individual Australians.

That the provision for daily fines be repealed to restore public trust in the Census. There could be a one-off fine of a nominal amount for failure to complete the Census with an exemption process for exceptional circumstances.

Retention

In the past the ABS says that “names and addresses have been destroyed at the end of Census data processing”.[7] The ABS 2015 PIA recommended that the ABS retain names and addresses from the 2016 Census. There was no recommendation to ever delete the names and addresses retained, and this is what the proposal appeared to be in very early 2016.[8]

[5] ACCC/ASIC Debt Collection Guideline available at https://www.accc.gov.au/publications/debt-collection-guideline-for-collectors-creditors
[6] See http://www.abs.gov.au/websitedbs/censushome.nsf/home/newsboard160823
[7] See http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacy?opendocument&navpos=130
[8] Page 25 of the ABS PIA 2015.

This proposal was changed to "4 years or less if no longer useful" after the start of a public outcry about the retention of names and addresses in early 2016.[9] The retention is to enable data matching and to allow for the creation of a unique identifier.

Recommendation 6
That the Act be amended to preclude retention of census or survey data collected under the Census and Statistics Act in a personally identifiable form by ABS or any other organisation.

Security

The ABS itself has reported a number of recent data breaches (14 since 2013)[10], and internal prosecutions. We also note that the OAIC is investigating possible security breaches with the online census form. The security of the Census data is critical.

Independent external audits should be required on a regular basis to ensure this highly personal information is safe. These should include the current and future threat level from re-identification of de-identified data, including data already released.

Recommendation 7
Independent external audits are conducted regularly to ensure the security of Census data is protected, including the de-identified forms which are released publicly under the assumption that the identity of the subject is adequately protected.

Use of data

This is a key concern. It is not transparent in any way how the ABS plans to use the personal information of Australians. A particular concern is that the ABS has not disclosed how it plans to use the linkage key (SLK). This was not covered in the 2015 PIA in any detail. We hope the Committee is able to shed light on this question one way or another, ideally by publishing the proposed uses of the SLK (or any other proposed unique identifier to be used) in detail.

Recommendation 8
That no Australian [or 'census data'] be subjected to a linkage key.

Recommendation 9
That the Act be amended to preclude names and addresses from being used for any purpose other than administering the data gathering process, and to mandate their destruction as soon as that purpose has been satisfied.

c) Arrangements, including contractual arrangements, in respect of the information technology aspects of the Census

No comment.

We note that other interested parties will likely be making submissions on this important issue.

We also note that there has been little transparency in relation to the most obvious cause of the site's failure, even if it had not been abandoned, namely under-provisioning of capacity to handle peak load, and under provisioning of DDOS protection services. The lack of transparency is a concern which we hope the committee remedies by requiring publication of all relevant documents. Many millions of hours of attempting users have already been wasted, which constitutes the largest financial loss of the night, albeit unpaid. Inadequate infrastructure and risk

[9] See http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacy?opendocument&navpos=130
[10] See https://www.theguardian.com/australia-news/2016/jul/29/australian-bureau-of-statistics-reports-14-data-breaches-since-2013

management provisions obviously can have an impact on personal information security and privacy rights related to secure handling of data.

d) The shutting down of the Census website on the evening of 9 August 2016, the factors leading to that shutdown and the reasons given, and the support provided by Government agencies, including the Australian Signals Directorate.

The APF notes that the ABS provided a series of confused, confusing and mutually inconsistent statements about the events on the evening of the Census.

The APF contends that public confidence in the capacity of government agencies to design and operate Internet-based schemes has been severely undermined in part by the failure, but even more so by the ABS' failure to provide an understandable, comprehensive and honest explanation.

The APF further contends that the Senate Committee's Report will fail to satisfy the need, to re-build public trust and confidence, unless it provides the understandable, comprehensive and honest explanation, which neither the ABS nor the government have provided.

> ***Recommendation 10***
> *That the Committee's Report provides an understandable, comprehensive and honest explanation of the events surrounding the close-down of the Census website, and the rationale underlying it.*

e) The response rate of the Census and factors that may have affected the response rate

The APF has no doubt that many people in Australia have either refused to complete the Census, refused to give their name, misspelt their name, and/or given partial or deliberately inaccurate responses, due to privacy and/or security concerns. The quality and integrity and therefore the utility of the 2016 Census results will inevitably be questionable.

> ***Recommendation 11***
> *That the Committee should receive independent expert advice on whether the quality of the data collected in the 2016 Census is such that it can be used reliably, and the Committee's Report should on that basis make a recommendation whether the data should be destroyed.*

f) Privacy concerns in respect of the 2016 Census, including the use of data linking, information security and statistical linkage keys.

Is name compulsory?

In the past, the ABS has collected name and address and then destroyed it. The ABS prosecuted no one for failure to provide their name. For Census 2016, this position changed.

On the ABS website it states[11]:

> Are names and addresses compulsory in the Census?
>
> Names and addresses have been collected in every Census.
>
> Names and addresses are specified in the Census Regulations as Statistical Information, like all other Census topics. This requires the ABS to collect this information as part of the

[11] See http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacy?opendocument&navpos=130

Census. The requirement for all topics, including names and address, on the Census forms to be filled completely and accurately is consistent with 105 years of Australian Census practice, the Census and Statistics Act 1905 and legal advice to the ABS from the Australian Government Solicitor. The only exception is religion, which the legislation specifies is optional.

The above information is misleading, given that name is arguably not compulsory, and in the past has not been used as it is intended to be now. The aim is to deny and downplay the significance for the change, despite the findings of the 2005 PIA that it was significant. Misleading the Australian public is unacceptable and should not be tolerated.

The ABS has apparently obtained legal advice from the Australian Government Solicitor (as noted above) but this advice has not been released. This advice should be immediately made public. It is not tenable to assert that one has to trust, unseen and unexamined, the conclusions of secret legal advice.

The APF contends that name is not compulsory under the Act and Regulations. We contend that the AGS is incorrect in its interpretation. We also contend that this is such an important issue that the legal advice should have been released as part of the consultation on the changes so it could be tested.

We note that many professionals have also questioned the above interpretation by the ABS. Dr. Caroline Henckels has argued that "name" cannot be a statistic and accordingly cannot be compulsory. Her argument is set out in full on the blog for the Castan Centre of Human Rights[12]. This argument is also made by former ABS Australian Statistician Bill McLennan, in a letter published on our web site and elsewhere, and not answered substantively by ABS.

Despite these clear arguments disputing the ABS interpretation the legal advice has not been released and the issue is not resolved. Accordingly, many Australians went to complete the Census and were misled into believing name is compulsory when this is a highly contested legal point. In addition, it may be questioned whether there is a constitutional basis for the collection of names and addresses, and the constitutionally valid scope of the use of any such information so collected.

These points also have a profound impact on whether the ABS has complied with the Privacy Act.

Recommendation 12
That the ABS be instructed to publish all relevant legal advice.

Recommendation 13
That, if a tenable legal argument exists to the effect that ABS can demand name and apply sanctions for its non-provision, the law be amended to ensure that no such power exists.

Privacy Act

The 2015 PIA states that the ABS has clearly committed to comply with the *Privacy Act*. This is obviously an absolute minimum.

Australian Privacy Principle 2 – anonymity and pseudonymity – clearly states that individuals must have the option of not identifying themselves or using a pseudonym. There are two exceptions to this principle:

1. The APP Entity is required or authorised by or under an Australian law to deal with individuals who have identified themselves or
2. It is impracticable for the APP entity to deal with individuals who have not identified themselves

[12] See https://castancentre.com/2016/08/06/do-i-have-to-provide-my-name-on-my-census-form/

The only arguable exception is the first exception which will depend on an interpretation of the law on whether name is compulsory. If it is not compulsory then the ABS is in breach of the Privacy Act. If so, then the Privacy Commissioner should take the appropriate proceedings against the ABS. (If it is found to be compulsory, then see our recommendations to change this, above.)

Recommendation 14
The Federal Privacy Commissioner investigate a breach of Privacy Principle 2 by the ABS

g) Australia's Census of Population and Housing generally, including purpose, scope, regularity and cost and benefits

There have been many reports over the years of unwelcome harassment of individuals by the ABS in the conduct of the many other surveys undertaken by the Bureau, such as the Household Expenditure survey. There have been reports to us this year from people no longer trusting ABS in light of the intrusive change to the Census, and unwilling to be forced into the other surveys.

APF submits that relevant recommendations in relation to the Census should also be applied to the ABS' other surveys. In particular there should be:

1. A process in place to apply for exclusions from this process on the broad grounds of hardship (for example illness, excessive time cost, obligations to a small business, family etc.)
2. That the ABS be required to give participants the option of completing the survey at a convenient location that is not their home
3. Develop guidance to prevent harassment and threats
4. Require their supervisor and regional manager to be identified by field officers, who are in the Census often temporary and with no permanent link to ABS.

h) The adequacy of funding and resources to the ABS

No comment. Other interested parties will likely make submissions on this important issue.

We observe that it has been suggested by some commentators that budget cuts have been one reason why the ABS has been moving in the direction of a significantly different role as a data aggregator, which has given rise to the 2016 Census problems.

The potential for increased monetisation of data, as has led to privacy abuses in industry, appears to have been considered as a legitimate driver, without adequate consideration of the potential for projecting risks onto data subjects by giving downstream 'customers' more of what they want, which is often identified data.

i) Ministerial oversight and responsibility

The APF is concerned about the lack of Ministerial oversight of the Census. There have been a series of Ministers in quick succession, with little capacity to become familiar enough with the challenges to offer real oversight. There also appears to have been little scrutiny of the claims and direction of the ABS in its conversion of the Census from statistics to surveillance. The APF has written two letters to the Prime Minister[13] with no substantive response. The issues we have raised remain unaddressed by the Government and it is hoped this Inquiry may begin that process.

[13] First letter from APF to PM is at: https://www.privacy.org.au/Papers/PM-Census-160208.pdf and second letter: https://www.privacy.org.au/Papers/PM-ABS-census-APF-040816.pdf

If you have any questions please do not hesitate to contact the writers.

Yours sincerely



Kat Lane, Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay, Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile, Vice-Chair
0414 731 249
David.Vaile@privacy.org.au