Australian Bureau of Statistics

Canberra Office
ABS House
45 Benjamin Way
Belconnen ACT 2617

Phone 1300 135 070

Locked Bag 10
Belconnen ACT 2616

www.abs.gov.au
ABN 26 331 428 522

James Smith
foi+request-2123-be184ab4@righttoknow.org.au

FOI ref: 201617/26

Dear Mr Smith

RE: YOUR FREEDOM OF INFORMATION REQUEST

I refer to your email of 11 August 2016 in which you sought access to the following information under the *Freedom of Information Act 1982* (FOI Act):

- All documents in FOI request 201516/07 with the inclusion of all information which was previously redacted (as it was deemed irrelevant). Please exclude employee names for non-SES.

Response to your request

I am an authorised decision maker under section 23 of the FOI Act.

The ABS conducted an exhaustive search for documents for your previous FOI request (201516/07). In that decision, the ABS released 13 items to you, but redacted content deemed to be irrelevant under section 22 of the FOI Act.

In light of your new request under the FOI Act (201617/26), I have now reviewed the previously redacted content and of the 13 documents in scope, I have decided to give you further access, in part, to 10 items. The documents being released to you are at Attachment 2.

Statement of reasons

Redactions have been made to the documents for the following reasons:

Item 11 was previously provided to you with no content redacted under section 22 of the FOI Act. As a result, no further access will be granted.

I have decided that items 1-10, 12 and 13 contain personal information which is exempt under section 47F of the FOI Act. Section 47F provides for documents 'which would involve the unreasonable disclosure of personal information about any person' to be exempt. These documents contain information about the names of staff, which after consideration of the facts I have determined it would be unreasonable to disclose.

I have decided that items 1, 2, 3 and 4 contain information which exposes the 'thinking processes' of the ABS which is exempt under section 47C of the FOI Act. This information is exempt under section 47C of the FOI Act as it would disclose deliberation that occurred in relation to functions of the ABS.

I have decided that items 12 and 13 contain information that is exempt under section 47E (c) of the FOI Act. Release of this information would reasonably be expected to have a substantial adverse effect on the management and/or assessment of personnel by the ABS. This information does not include information previously released in response to your previous FOI request.

The exemptions above only apply if release of the information would also be contrary to the public interest.

I have decided that release of this information would, on balance, be against the public interest. Although it is true that the redacted information would likely enhance the scrutiny of government decision making and inform debate on a matter of public importance, release would also be reasonably expected to prejudice the ABS' ability to obtain confidential information. As the ABS' main business is obtaining confidential information from businesses and members of the public in order to create high quality statistics, I place a great deal of weight on this factor.

Charging or Waiving of Processing Fees

There is no charge for this request.

Internal Review of the Decision

Section 54 of the FOI Act gives you the right to apply for an internal review of the decision by the Australian Bureau of Statistics. Additionally you may request a review of this decision by the Information Commissioner. Details of both procedures involved in an application to review a decision are set out at Attachment 1.

If you have any queries on this matter please contact the ABS FOI Contact Officer at freedomofinformation@abs.gov.au or on (02) 6252 7203.

Yours sincerely

Samantha Palmer
General Manager
Governance, People and Culture Division
Australian Bureau of Statistics
12 September 2016

INFORMATION ON RIGHTS OF REVIEW

1. APPLICATION FOR INTERNAL REVIEW OF DECISION

If you disagree with our decision you have the right to apply for an internal review under section 54 of the FOI Act.

Application for a review of the decision must be made within 30 days of receipt of this letter.

No particular form is required but it would assist the decision-maker were you to set out in the application the grounds on which you consider that the decision should be reviewed.

Application for a review of the decision should be addressed to:

ABS FOI Contact Officer
Policy, Legislation and Assurance Section
Australian Bureau of Statistics
Locked Bag 10
BELCONNEN ACT 2617

OR

2. APPLICATION TO AUSTRALIAN INFORMATION COMMISSIONER (INFORMATION COMMISSIONER) FOR REVIEW OF DECISION

Section 54L of the Act gives you the right to seek a review of the decision from the Information Commissioner. An application for review must be made within 60 days of receiving the decision.

Applications for review must be in writing and must:

- give details of how notices must be sent to you; and
- include a copy of the notice of decision.

You should send your application for review to:

The Information Commissioner
Office of the Information Commissioner
GPO Box 5218
SYDNEY NSW 2001

AND/OR

3. COMPLAINTS TO THE INFORMATION COMMISSIONER

Section 70 of the Act provides that a person may complain to the Information Commissioner about action taken by an agency in the exercise of powers or the performance of functions under the Act.

A complaint to the Information Commissioner must be in writing and identify the agency the complaint is about. It should be directed to the following address:

The Information Commissioner
Office of the Information Commissioner
GPO Box 5218
SYDNEY NSW 2001

The Information Commissioner may decline to investigate the complaint in a number of circumstances, including that you did not exercise your right to ask the agency, the Information Commissioner, a court or tribunal to review the decision.

Attachment 2

Item no. 1 – Paper to the ABS Executive Leadership Group (ELG) meeting of 19 October 2015 – ‘Retention of Names and Addresses in the ABS’ and relevant attachments.

Executive Leadership Group

19 October 2015

Paper title: Retention of names and addresses in the ABS

Author area: 2016 Census Program [redacted]

Recommendations

1. ELG agree to the conduct of a Privacy Impact Assessment (PIA) of the following proposed changes to ABS Privacy Policy:

1.1 Permanent retention of addresses, using separation principles to separate from data file but be linked for approved purposes (para 11).

1.2 Retention of raw names as a data linkage resource only, using anonymised version of names for data linkage (paras 12 to 28).

2. ELG agree that the PIA be used as the primary vehicle for external engagement and communication in relation to retention of Census identifiers (pars 29 to 33).

3. ELG note that there are and will continue to be a number of exceptions to the current policy in place, with ABS applying option 4 or similar arrangements in a number of situations.

Background

1. In accordance with ABS policy, personal identifiers (such as names and addresses) are deleted from the Census, as well as most surveys, after the completion of processing. Names and addresses have been used for approved statistical purposes during this "processing period" in data integration projects associated with the 2006 and 2011 Census (see Notes Link).

2. There is a widely held view within ABS that continuing to operate under such restrictions will be a significant barrier in meeting both statistical and operational aspirations.

3. The Census Program was asked to investigate this issue on behalf of the organisation. An exposure draft paper was presented to ELG in December 2013 (see Notes Link). [redacted]

Benefits and privacy risks

4. The retention of names (or a form of names) and addresses would provide a benefit to the ABS and the wider community as it would:

- enable higher quality linkage of survey, administrative and census datasets (improved linkage rates as well as successfully linking amongst traditionally hard to link groups, such as Aboriginal and Torres Strait Islander peoples);
- support a range of organisational efficiencies, such as the development of the ABS Address Register, improved sampling, imputation, and provider management;
- support more flexible, geo-spatial outputs; and
- support our desire to be the premium data integration service in the NSS and encourage greater sharing of government information for statistical purposes.

5. In particular, the emergence of data integration as a key strategic direction for the organisation, together with whole of government priorities for public sector data management, has increased the motivation for reviewing the current policy. ABS data integration activities can be expected to expand significantly in the coming years as ABS gains access to additional key, nationally important, administrative datasets. Maximising their utility will result from the ability to conduct multiple high quality linkage projects, through linking amongst administrative datasets, business surveys and the Census. This is a critical enabler for the transformation of both people and economic statistics.

6. The key risks of extending ABS policy on the retention of names and addresses relate to the potential for loss of trust from providers due to privacy concerns or breaches, leading to a reduction in response rates to ABS collections. Making the public commitment to delete such information has been seen as a powerful strategy to alleviate any concerns over privacy and confidentiality, whilst also reducing the risk of accidental or malicious disclosure.

Focus group testing

7. Focus group testing was conducted to explore privacy concerns and issues related to the retention of names and addresses by the ABS. A summary of the focus group testing results is in Notes Link. The key themes that emerged were: the need for a public good; the importance of quality information for good decision making; transparency of ABS retention and use of personal identifiers (a requirement of the new Privacy Act); and security.

8. A majority of participants believed that an anonymised name offered a greater degree of protection for the security and privacy of individuals, and represented a lower risk than raw names. A key concern in retaining raw names related to the belief that personal identifier information could or would remain appended to survey or other government data. In the focus group it was not possible to explore the use of separation principles for names and addresses, and it is therefore possible that being able to effectively articulate the use of separation principles may mitigate these concerns to some extent.

9. The retention of addresses appeared to be generally acceptable to participants, although it was noted that there could be some sensitivities as an address could be seen as more personal than a name (as it relates to a physical location rather a name which could be seen as something more abstract).

10. The testing suggested that transparency by the ABS and consistency of the ABS' behaviours between policy and practice are more important to providers than what decision ABS makes on name and address retention.

Options and recommendations

11. Retention of addresses - The Census program recommend changing the ABS policy such that addresses (and their associated geocodes) be retained permanently - with the use

of separation principles. Mesh Blocks would continue to be retained on the data file(s) so they are "geospatially enabled". This has significant statistical and operational benefits, through supporting the improvement of geospatial statistics, the ABS Address Register, and other operational efficiencies. This is seen as a **medium privacy risk** (likelihood of this being a broad provider concern - possible, severity of impact of this concern to ABS - minor), and is supported by the findings of the focus groups.

12. Retention of names - four options have emerged through internal consultation and focus groups:

Option 1: No change to the current ABS policy;
Option 2: Destroy raw names but retain an anonymised version of names;
Option 3: Retain raw names as a data linkage resource only, using anonymised version of names for data linkage; or
Option 4: Retain and use raw names.

Option 1: No change to the current ABS policy

13. As explained above, this option would severely constrain ABS aspirations in relation to data integration and potentially damage the ABS' reputation as a premium data integration provider.

14. The privacy risk of this option is rated as **medium** (likelihood - possible, severity - moderate), but is consistent in nature to previous Census and current ABS approaches. The risk to ABS outcomes of this option is rated as **extreme** (likelihood - almost certain, severity - major). For these reasons, it is not considered a viable option.

Option 2: Destroy raw names but retain an anonymised version of names

15. Option 2 is the permanent retention of anonymised (encoded), unique statistical linkage keys, which are based on names — with the use of separation principles, whereby the name-based statistical linkage key is removed from, but able to be linked to, the data file(s). Raw names would still be used during the processing of Census data, including for the conduct of the Post Enumeration Survey and the production of Aboriginal and Torres Strait Islander life expectancy estimates (accuracy of linkage with anonymised name is yet to be proven for this population group and thus maintaining consistency with previous approach is recommended until it is determined whether or not anonymised name is sufficient). Raw names would be deleted after the completion of this work.

16. This approach provides a balance between additional benefit and risk management, but it may still limit statistical objectives to some extent. The use of anonymised names in data linkage can generally provide linkage rates almost as high as with raw names, however in some specific cases (e.g. Aboriginal and Torres Strait Islander people and some migrant populations) this has not yet proven to be the case. This option provides the ABS with only one opportunity to generate a set of linkage keys and thus restricts the capacity to review, revise or improve on the encoding in the future to meet new challenges or new opportunities.

17. The benefits of option 2 include:

- continuing the public message that we don't retain names which should not result in any risks to Census related to privacy; and
- considerably improved linkage rates over linkage using meshblock, date of birth and other characteristics only.

18. The risks of option 2 include:

- privacy risks of a change to public messages around retention and greater use of name based information (and therefore a potential impact on Census participation), albeit with the 'reassurance' that we delete names (**High risk**: likelihood - possible, impact - major);
- loss of flexibility to, and potential opportunities that would be accessed through, generating new linkage keys in the future to meet new and changing needs (**High risk**: likelihood - almost certain, impact - moderate); and
- potential loss of business, and ABS reputation, as a premier integrator of government data — external partner agencies may see as ABS unnecessarily constraining itself and therefore constraining whole-of-government data integration projects through not allowing for the highest possible linkage quality (**Medium risk**: likelihood - possible, impact - moderate).

Option 3: Retain raw names as a data linkage resource only, using anonymised version of names for data linkage

19. Option 3 is the permanent retention of raw names, however these would be permanently separated from the remainder of the collected data file (ie separated from the other characteristics of the individual). The raw names would be retained in a separate file. Anonymised versions of names would be generated from the raw names and then recombined with the data file in order to allow data linkage.

20. The name file would be used as a resource for data linkage research and practice, forming part of the foundational infrastructure for ABS' data linkage activity.

21. The use of separation principles and security would be critical in mitigating the privacy risks in terms of the accessing or release of identified data, and helping to assure the public that the information they provide to the ABS would remain private and confidential. Under this option, the public could be assured that their name is separated from our Census and other data files, and strict security mechanisms are put in place to ensure that staff can not access both a person's name and their survey responses.

22. It would be important to highlight the public good element of retaining names, that is, that it would contribute to better social and economic outcomes for Australian's through having higher quality, richer information for decision making and policy development and evaluation - and that this retention will only be used for statistical purposes as protected by legislation.

23. The benefits of option 3 include:
- being able to provide public assurance of the separation of names from other characteristics that are collected ("names are removed from the Census data set and are never added back");
- ensures strong alignment between ABS policy and statistical intentions/aspirations;
- enabling higher quality linkage than under option 2; and
- providing flexibility to continue to research and improve on anonymised data linkage mechanisms.

24. The key risks of option 3 are that:
- it leads to privacy concerns and reduced trust in the ABS, and in particular, putting at risk the level of participation in our collections. There is the potential for a public backlash (including from the privacy lobby), which would need to be carefully managed (**High risk**: likelihood - possible, impact - major);

- the use of anonymised names for data linkage lead to a statistically significant reduction in data quality in some instances (**Medium risk:** likelihood - unlikely, impact - moderate); and
- it leads to concerns from clients or other custodians that the quality of data is being compromised through the us of anonymised data linkage mechanisms (**Medium risk**: likelihood - possible, impact - moderate).

Option 4: Retain and use raw names.

25. Option 4 is similar to Option 3, however there would be no commitment to not link raw names back with collected characteristics and raw names would be utilised directly in data linkage.

26. The retention of names for direct use in linkage gives ABS the ultimate flexibility and is the approach taken in Statistics New Zealand. It is not clear, however, to what extent there is a requirement to link with raw names beyond the two current exceptions cited above (Census Post Enumeration Survey and Indigenous Mortality Project).

27. The key benefit of option 4 is to achieve all of the outcomes highlighted in option 3 in relation to data linkage, but without any potential compromise of linkage capacity or ABS reputation as the premium data integrator.

28. The two key risks of option 4 are:
- it leads to privacy concerns and reduced trust in the ABS, and in particular, putting at risk the level of participation in our collections. There is the potential for a public backlash (including from the privacy lobby), which would need to be carefully managed (**High risk**: likelihood - possible, impact - major); and
- it leads to accidental or malicious disclosure of identifiable data (**High risk**: likelihood - unlikely, impact - severe).

Privacy Impact Assessment

29. The approach to address retention and data integration for previous Censuses, and our decisions on all new data integration projects have been informed by the conduct of a privacy impact assessment (PIA). The conduct of a PIA to consider the application of this change in policy on the Census is considered the best practice to assess the potential impact and appropriateness of this change on privacy in order to inform a final decision by ELG.

30. Whilst an external PIA was conducted in 2005 in relation to Census retention and integration, it is proposed that a PIA for these changes for Census 2016 is conducted internally, consistent with our practice with data integration projects and leveraging the experience and knowledge we have built since 2005.

31. There is a need to engage with key stakeholders over any changes to the ABS policy, particularly given the rapidly approaching 2016 Census. [redacted] The Census Nature and Content publication (August 2015) and Census Products and Services (October 2015) both had an increased emphasis on Census data integration and indicated a potential change in position on retention and use of names and/or addresses collected in the Census.

32. When a final decision is made, it is proposed that the PIA is published on the ABS website along with the report from Colmar Brunton Social Research on the focus group research on public attitudes to data retention and integration by the ABS. It would be ideal for this to quickly follow the release of the 'Trust in ABS' survey.

33. Engagement in relation to changing ABS policy in relation to the retention and use of names and addresses should ensure that key stakeholders are aware of ABS plans.

Executive Leadership Group Meeting

Monday 9th December

Retention of personal identifiers in the ABS

[redacted] **Census Branch**

Purpose of the paper

The purpose of the paper is to:

1. raise the key issues that need be considered in relation to the retention and use of personal identifiers;
2. initiate ELG discussions on the retention and use of personal identifiers in the ABS, and in the first instance consideration of the 2016 Census of Population and Housing; and

[redacted]

Key issues

1. In accordance with ABS policy, personal identifiers (such as name and address) are deleted from Census, as well as most survey and administrative files, after the completion of processing.
2. The retention of personal identifiers would provide a benefit to the ABS (and wider community) as it would enable high quality linkage of the Census dataset with other survey, administrative and Census datasets. Data integration is a key strategic direction for the organisation.
3. The retention of personal identifiers would support the development of the ABS Address Register and its use as a means of improving organisational efficiency through better sampling, and more effective and efficient provider contact. It would also support broader ABS organisational efficiencies.
4. There is a risk that privacy concerns around retention of personal identifiers would reduce trust in the ABS and / or reduce the level of voluntary compliance with ABS collections. Retention of personal identifiers increases the risk of breaches of confidentiality and privacy through disclosure.

Consultation undertaken in preparing this paper

1. Consultation has included the Data Linkage Centre and Data Integration NSC, Geography, National Tax Data and Business Demography. A draft of the paper was presented at the Data Integration Steering Committee (DISC) (including representatives from PLASS, OOTSEE, EESG and MDMD).

Action required by ELG

It is recommended that ELG:

1. consider the issues raised in the paper;
2. provide some preliminary views on the retention of personal identifiers; and
3. endorse the further exploration of the retention of personal identifiers, including undertaking public consultation.

Retention of personal identifiers in the ABS

1. Introduction

1. The ABS has traditionally collected various forms of personal identifiers in our collections, this has generally been only required (and therefore used) for operational reasons. The destruction of these identifiers after processing, a step in a traditionally linear statistical production process, was a way of clearly protecting the privacy of the provider and provider perception of the ABS, with only limited impact on potential benefits.

2. The increase in the potential for data integration through improved methods, processes, technology and availability of rich administrative datasets has increased the value of personal identifiers, as these identifiers enhance the ability to accurately link records between data sets.

3. Personal identifiers are also critical to enabling the ABS to implement more efficient data collection operations including improved targeted sampling and effective interviewer-less contact of respondents.

4. Considering the benefit of retention of personal identifiers, there is a need for an organisational discussion and examination of ABS policies regarding the retention and use of personal identifying information to ensure that we have the right balance between benefits and risks. Whilst there are some different considerations for Census, surveys and administrative datasets, it is important for the issue to be considered holistically.

5. The issue of personal identifier retention has been raised in a number of fora recently, in the context of administrative data, the statistical spatial framework, household survey operations, the Census, and data integration (see Attachment 1 for the relevant papers). Given the Census is central to many of the current and potential data integration activities, as well as being the most high profile ABS collection, at the August 2013 steering committee meetings for the Statistical Spatial Framework and Data Integration Steering Committee it was agreed that Census Branch would take the lead in progressing this issue to ELG for discussion and decision, with a focus on considering the issue first for the 2016 Census.

6. Decisions relating to the retention of names, addresses and other personal identifying information have potential impacts on multiple Census goals, namely:

- *improve the quality of data collected by the Census (including relevance, timeliness, accuracy, coherence, interpretability and accessibility)*
  Retention of personal identifiers could improve the value of Census data through data integration and linking, which would enable new products as well as

improving quality of Census data through quality assurance and improving imputation.

- *maintain and make targeted improvements to the coverage of the population overall, including at the small area level and for specific population groups*
  Retention, or more specifically concerns about retention and data use, could impact respondent behaviour and create a negative impact on the Census response rate, coverage and cost of operations.
- *contribute to the sustainability of the Census and the wider ABS through the ABS 2017 Program*
  Retention would provide a more valuable Census data set for other areas of the ABS and significantly increase the quality and value of the ABS Address Register. The retention of 2016 Census data would be valuable in the development and conduct of the 2021 Census.

7. The purpose of this paper is to:

1. raise the key issues that need be considered in relation to the retention and use of personal identifiers;
2. initiate ELG discussions on the retention and use of personal identifiers in the ABS, and in the first instance consideration of the 2016 Census of Population and Housing; and

[redacted]

2. What are personal identifiers?

8. The ABS policy refers to "...names, addresses and other identifiers of individuals...".

9. The Privacy Act defines personal information as "...information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

10. While some data items are likely to represent a greater identification risk in their own right, the likelihood of identification of an individual will depend on the number of data items and their nature. In the Census context, the main personal identifiers of relevance are name; address (as well as other address-coded geographic information such as meshblock and geocode); and date of birth.

11. Names and addresses collected in the Census are not retained, however date of birth, meshblock (since 2006) and a "one to many" encryption of name (since 2011) are retained.

[redacted]

[redacted] the focus of this discussion, in terms of changing practice in the Census, relates to names and addresses. Names and addresses are considered the most 'sensitive' in the context of privacy, as well as holding the most intrinsic value in the data integration context. ELG views on the range of potential 'personal identifiers' relevant in this context are welcomed.

3. Current ABS policy

14. The current ABS policy in relation to retention of personal identifiers is found in the Policy and Legislation Manual (Policy 04, Privacy, subsection 01 Privacy Act 1998), and states that:

> "It is ABS policy that name, address and other identifiers of individuals must be deleted from collected survey and administrative files as soon as practical after processing, unless there is a business need approved by the Australian Statistician."

15. The ABS policy, as currently applied, has a range of potential limitations:

- the default position is that personal identifiers are not retained unless Statistician exemption is approved;
- it does not differentiate between different personal identifiers which may have different uses and risk profiles and therefore groups all personal identifiers under one approach;
- it presumes the area undertaking the data processing is in a position to assess whether there is an immediate business need or an identified future business need;
- it precludes the ability for meeting a business need which is identified after processing is complete; and
- is orientated around the traditional survey cycle of processing as a once off event in a linear process (rather than our future information management approach).

16. While the current ABS policy requires names and addresses to be deleted once 'processing is complete', the notion of a defined (and finite) end-to-end processing period is no longer as meaningful or relevant. The statistical system is necessarily becoming more complex, with an increasing focus on information management rather than collections. Census, survey and administrative datasets are increasingly being viewed as enduring statistical assets, with potential uses far beyond the end of what might be viewed as the traditional processing period which ends when initial survey results are released.

17. When considering the notion of processing in the Census context, the SLCD provides a useful example. The SLCD is part of the suite of Census products, not an add on to the Census, so it could reasonably be regarded as part of the processing of the Census. In the SLCD context, processing of one Census could be seen as incomplete at least until it has been linked to the subsequent Census. Data integration is increasingly seen as a part of the future of Census processing.

4. Opportunities - Value proposition of change

18. There are a number of business benefits for the retention of personal identifiers. Broadly, these relate to:

- statistical data integration;
- enhanced geospatial enablement of statistics;
- productivity and efficiency; and
- reducing provider burden.

19. There is also a strong element of public good that relates to the benefits, either in relation to providing government and the community with a greater range of information which can be used to inform on important social and economic policy challenges, as well as through more efficient use of government resources.

4.1 Statistical data integration

20. The emergence of data integration as a key strategic direction for the organisation has increased the motivation and urgency for the review of the current policy on the retention of personal identifiers. ABS data integration activities can be expected to expand significantly in the coming years as ABS gains access to additional key nationally important administrative datasets. Maximising the utility of these datasets, as well as of the Census and survey datasets, will result from the ability to conduct multiple high quality linkage projects, through linking multiple administrative datasets, linking administrative datasets to surveys and/or the Census, and linking the Census to surveys. Name and address information has the potential to markedly improve the quality of data linkage.

21. Through the launch of the ABS' Information Management Transformation Program (Pink, 2000) and now ABS2017, the business of the ABS is changing to be more focussed on information management across both collection based and administrative data. In a modernised operating environment, we need to stop considering collections as separate, stand-alone data sources and focus our business on considering information needs holistically and providing information solutions based on whatever sources or sources that are available. This will involve iterative processing of the range of data sources held by the ABS, and in many cases will require the ability to integrate (link) these data sources, in order to maximise their value. While we may not know all of the potential future uses of all the datasets the ABS holds, the retention of some or all personal identifiers would enable us to to be in a position to meet those future needs as they arise.

22. The Census Data Enhancement program (for 2006 and 2011) has been a huge success, with a variety of valuable data integration projects having been undertaken. For example, the Statistical Longitudinal Census Dataset, Migrant Settlements project and Indigenous Mortality Study. It is important that ABS build on that success for the 2016 CDE, as well as more broadly across the ABS, through maximising the range and value of data integration projects that are able to be undertaken. Many of the CDE projects undertaken in 2006 and 2011 have focussed more on linkage quality, so for 2016 the focus will increasingly need to move to statistical outputs, and this would be supported by the retention of personal identifiers in the Census, administrative and survey datasets.

23. Statistical data integration offers the potential to produce new data products, as well as enrich existing data products. There are many administrative datasets that are likely to have considerable statistical value. In addition to the Personal Income tax data which has already been used in data integration projects, future data integration projects could include the use of FaHCSIA welfare payments data, Centrelink unemployment benefits data,

Medicare and Pharmaceutical Benefits Scheme data, Australian Immunisation Register, the AEC electoral role, and other nationally important datasets.

24. The assurances provided to the public around data integration have been successful in maintaining public trust, but this has come with some trade-offs. We have limited the program to linkages that were declared before the Census and limited the program to linkages that could be conducted during the processing period of the Census. The use of bronze linkage processes (linking without name and address) has meant that the Statistical Longitudinal Census Dataset is not as complete as it could be, and some groups like Aboriginal and Torres Strait Islander people and people who move addresses are under-represented in the dataset.

25. The ABS provides an effective and safe environment for data integration. As an Accredited Integrating Authority under the interim Commonwealth data integration arrangements, ABS has the experience and infrastructure to undertake high risk data integration projects, as well as a high level of Community trust. There are many data integration activities that only the ABS is able to undertake, i.e. those that relate to information collected under the Census and Statistics Act.

26. As the future of the population and social statistical program continues to evolve, it is likely that the Census will increasingly become central to population and social statistics, i.e. Census as a 'spine' for the population and social program. This will only increase the need for, and benefits of, statistical data linkage with the Census. The use of Gold Linkage (i.e. using Names and Addresses) would ensure maximum value for what is already one of the most valuable statistical assets the ABS holds.

4.2 Enhanced geospatial enablement of statistics

27. The Spatial Statistical Framework aims to provide a consistent and common approach to geospatially-enabling statistical and administrative data. The framework is the key strategy in achieving the NSS priority of enabling statistical information to be integrated with location information.

28. The inclusion and retention of a geocode and a geographical unit on unit record files will greatly enhance the ability of the ABS to produce consistent geospatially enabled statistical outputs. This will simplify geospatial analysis of ABS statistics and allow geography to be used to facilitate integration across data sources of aggregate level statistics. The inclusion of geocode information will also ensure flexibility into the future. Geocodes will allow the ABS to produce statistics for new or changed geographies and, potentially, for a wider range of geographic boundary types.

4.3 Productivity and efficiency

Development and maintenance of an Address Register

29. The Address Register will be critical to driving efficiency in ABS data collection activities. The initial development of an accurate Address Register requires the retention of collected dwelling address information.

30. The Address Register is intended to be an up-to-date and comprehensive list of all physical addresses in Australia, which supports collection activity for the 2016 Census of Population and Housing and other ABS household surveys. The Address Register will store a list of mailable and locatable addresses for every land parcel in Australia, including but not

limited to, residential, business and commercial buildings which can be used by survey areas to extract survey frames.

31. The Geocoded National Address File (GNAF) forms the basis of the address register, however GNAF is neither complete in its coverage, nor does it hold sufficient information on each address. To fully meet our objectives, the address register needs to be extended with additional addresses captured through the 2016 Census, as well as be populated with characteristics of these dwellings.

Efficiencies in survey sample design

32. The retention of personal identifiers would also enable more efficient survey sampling through the use of 'selective sampling'. For example, retaining information that allows us to understand that people (a person) with a certain characteristic of interest from a social policy/survey perspective is associated with a particular address, thus enabling, for example, targeted (and therefore more efficient) sampling in indigenous surveys, health surveys, etc.

Response rates

33. The retention of personal identifiers will be crucial in providing information to enable adjustments in household surveys with lower response rates (i.e. adjusting for non-response). Missing data can be imputed (or weights adjusted), which would reduce the cost of pursuing the last few percent of response rates. This would also allow the possibility of reducing target response rates in household surveys as an efficiency move.

Development of consolidated lists of data items as a corporate tool for name and address repair and standardisation

34. The Analytical Service Data Linking Team is working to develop a corporate tool to support name and address repair and standardisation, which would derive frequencies of key data items (e.g. given and surname, age, street and suburb name, country of birth etc.) using a variety of different administrative data files. This information would then be retained in a central repository, and used as a shared corporate resource by internal (and possibly external) clients engaged in record linkage.

35. The success of this project does assume that name and address information can be stored (separately) for the long term by the ABS, as the files would contain frequency information of names by year of birth and country and street address by suburb. The development of such a corporate tool is fundamental to research into record integration methodologies including the development of robust one-way encryption algorithms.

Efficiency of making contact with respondents

36. The implementation of self-enumeration electronic forms has removed the need for interviewer visits to be conducted for all households, however this relies on being able to make contact with households through other methods. The retention of names, addresses or other contact information increases the likelihood of the success of this contact by allowing the ABS to 'personalise' interactions with respondents, rather than addressing correspondence to 'The Householder'. However it is possible that some people may find it intrusive that ABS knows their name.

<u>4.4 Reducing provider burden</u>

37. Increased and improved statistical data integration also has the potential to reduce respondent burden, as some current and future data gaps will be able to be filled through integrating datasets rather than conducting surveys, or through being able to reduce the sample sizes or content of existing surveys.

5. Threats, risks and issues relating to change

Risks and issues relating to privacy, confidentiality and trust of providers

38. The retention of personal identifiers such as name and address is not precluded under the Census and Statistics Act, nor the Privacy Act.

39. The Census and Statistics Act 1905 states that information collected under that Act will be kept confidential. The Privacy Act places a number of requirements on Commonwealth agencies when collecting, storing, using and disclosing personal information. Under the Privacy Act, the collection and dissemination of personal information is limited to that which is core to the business needs of the agency. Personal information must be stored securely to prevent its loss or misuse. When collecting personal information from individuals, Commonwealth agencies are also required to do what is reasonable to ensure that the individual is made aware of the purpose for which the information is being collected.

40. It is important to note that from March 2014, the Privacy Amendment Act 2012 comes into effect (replacing the Privacy Act 1988). The Privacy Amendment Act includes a set of new, harmonised, privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs). They will replace the existing Information Privacy Principles (IPPs) that currently apply to Australian Government agencies and the National Privacy Principles (NPPs) that currently apply to businesses (see the OAIC website).

41. The Office of the Statistician and External Engagement (OOTSEE) is coordinating the implementation of these mandatory privacy changes across the ABS, including undertaking a review of the ABS privacy policy. The implementation process will consider a range of issues, such as the interactions between the Privacy Amendment Act, with its provisions for individuals to access and correct personal information held about them by an agency (as well as an agency having responsibility for ensuring that the personal information it holds about individuals is accurate, up-to-date, complete, relevant and not misleading), and the Census and Statistics Act.

42. The ABS strictly maintains the secrecy of all information provided under the Census and Statistics Act 1905. The answers provided are treated confidentially and no information is released in a way that would enable a person, household or business to be identified. This would continue to be the case if the ABS retained personal identifiers, however, the retention of personal identifiers would change the ABS' risk profile in relation to disclosure or inappropriate use. ABS would need to ensure that policies, processes and infrastructure are adequate to protect against this change in risk.

43. The ABS policy to delete personal identifiers is part of the ABS strategy to maintain the trust of providers. Making the public commitment to delete such information has been seen as a powerful strategy to alleviate any concerns over privacy and confidentiality, and ensure ABS is transparent about the use of personal information. Clearly articulating the specific uses of personal information before deleting is also a key component of the strategy to

manage risk. As noted above though, it does preclude their future use, no matter how important or worthwhile that potential use may be.

44. While the perception that personal information may not be secure would be a concern, the 'worst-case' scenario would be if there was a privacy breach with personally identifying information entering the public domain. This could result in a significant loss of confidence in the ABS. It should be noted that this risk already exists, given that personal identifiers are currently retained for the 18 month processing period of the Census.

6. Change options

45. The consideration of the ABS preferred approach, and thus appropriate policy, for retention of personal identifiers needs to consider a number of different aspects which have an impact on both the level of risk that the ABS is exposed to, as well as the benefit provided by the retention. The aspects that need to be considered include the source of the data (i.e. Census, survey or administrative), the specific identifier to be retained, the method of retention, the location of retention, the tenure of retention and the purpose/use of the retained data.

What personal identifiers could be retained, and how

46. The identifiers retained are likely to have significant impact on the potential benefit achievable. The retention of both names and addresses (including geocodes) would clearly have the most value. However, there are other 'fall-back' options that might still provide some benefit with less risk. The retention of addresses only is likely to be less of a privacy concern, but would still provide some of the benefits noted above (e.g. spatially enabling datasets, AR maintenance and efficiencies in sample design). To realise the full benefits though, names and addresses would be required. For example, the retention of both names and address was required by the CDE Indigenous Mortality Study linkage project.

[redacted]

48. Personal identifiers can be retained in a way that provides additional protection to privacy. For example, we could undertake a 'one-way' encryption of Names (or Names and Addresses) to create unique Statistical Linkage Keys and retain these, rather than retaining actual names. It is possible that this could satisfactorily meet some requirements around high quality data linkage, but without necessarily permanently retaining all personal identifying information. A one to many hash encryption code was stored from the 2011 Census to assist with SLCD linkage to the 2016 Census but this is a very coarse grained encryption mechanism in which about 40,000 people in the population share the same code.

How personal identifiers could be stored, and for how long

49. The ABS would be able to continue to meet its obligations in ensuring the privacy and confidentiality of respondents information even if it were to retain personal identifying information. As an Approved Integrating Authority, ABS is well placed to undertake safe storage and use of personal information.

50. Any retention of personal identifiers would need to be supported by secure storage, using the data integration separation principles. While the personal identifiers could be

retained on the data file, it may be prudent for them to be stripped off the data file, and be retained in a secure location, separate from the data, with a concordance to enable future secure data linkage. This is the approach used in New Zealand and Canada (see Attachment 2). Having strong protections on who can access the personal identifiers, and under what conditions, may alleviate or at least lessen some of the privacy concerns.

51. Consideration would also need to be given to the length of time the personal identifiers are retained. The current approach is to retain temporarily, for a period that represents the traditional view of 'processing'. The length of time personal identifiers are retained could still be tied to the processing period, but based on a modernised view of processing which would involve a longer time span thus enabling a greater range and timeframe of uses. For example, in the Census context, the period of processing for one Census could be extended to encompass the period up to the subsequent Census, to facilitate the production of the next iteration of the SLCD.

52. Alternatively, the personal identifiers could be retained for an (extended) defined period (defined based on the data source, and use/potential use of the identifiers from that source), or retained permanently.

Use of personal identifiers

53. The uses made of personal identifiers would need to be closely managed. There should be a clearly articulated approval process which would apply to the use of this information, for example, projects proposing to use personal identifiers from the Census, or any other source, would need to be approved by the Australian Statistician and be made public. This would also involve delineating the different types of uses, e.g. whether for operational purposes or for data linkage purposes.

7. Where to from here

[redacted]

How would we test community acceptance/attitudes to the retention of personal identifiers in the Census?

56. Across many aspects of people's lives, the collection and retention of personal identifying information is now a matter of course, as such information is necessary to enable the 'collector' to meet their core functions (e.g. welfare payments, service delivery, banking, etc.) or is an integral part of the medium (e.g. social media). While there will always be some apprehension around privacy, it could be argued that the community is more or less used to providing personal information in a variety of contexts, and in fact expect it. Notwithstanding this, there is still some evidence of public discomfort and mistrust around how their personal information is used. The issue may therefore be less about whether personal identifiers are retained, and more about what use is made of them, and by whom.

57. It will be important to gain an up to date understanding of community views on the retention of personal information. A number of focus groups were held in 2010 to assess trust in the ABS and attitudes towards the Census Data Enhancement proposal for the 2011 Census. The focus group found that there was a strong level of trust in the ABS (considerably higher than for other government agencies). It also found that the public trusted the ABS commitment to never release any data which could enable the identification of an individual (including in relation to data linkage).

58. While the results of the previous focus group testing are encouraging, this issue still needs to be carefully managed. A change in the ABS position would require public consultation to test community attitudes to the retention of personal identifying information, and its use in data integration\linkage activities. Further focus group testing or similar should be undertaken. This testing should consider Census as well as touching on the broader ABS perspective.

59. The timing of any public consultation would also need to be carefully considered, as it could have the potential to affect Census operations. As a result, any consultation would need to separated from the conduct of the Census by a significant time period. The testing could also be undertaking in consultation with focus group testing for the CDE given the strong links. Any change to ABS practice with respect to personal identifiers in the Census would need to be communicated to the general public, e.g. through the planned 2015 Information Paper on nature and content for 2016 Census.

61. There is a need for public transparency in what ABS is doing with personal identifiers such as name and address, and a clear articulation of the reasons and benefits to the community.

62. There are a number of areas that ABS may want to test/understand, including:

- public understanding of what ABS currently does, or doesn't do, with their personal information (as a baseline);
- ABS trust rating;
- community attitudes to different protection mechanisms, and different public messages - e.g. the extent to which ABS retaining an 'encrypted' name rather than

the name itself, or nature of the storage personal information, would alter privacy concerns;

- community attitudes to various potential uses of personal identifiers (e.g. in data linkage activities) as opposed to the retention itself;
- effectiveness of a range of different communication strategies - i.e. if the policy were to change, how to best articulate to the public what the ABS position is; and
- public sensitivity to a negative campaign, and reactions to ABS responses - i.e. how would a negative public campaign impact their support for the Census.

63. ELG views on what consultation should take place are welcomed, in particular what is the level of comfort in putting into the public domain the possibility of retaining personal identifiers in the Census at this time. ELG are also encouraged to identify if there are currently any 'no go' areas.

Next steps

64. A strategy for any consultation process will need to be developed shortly, including identifying the timing of engagement with key external stakeholders (e.g. Privacy Commissioner), and mapping out the work that will be required both prior to and subsequent to any consultation (e.g. further review of ABS policies in relation to the new National Privacy Principles, specific evaluation of the benefits and risks associated with retention across the different data sources and activities and for different identifiers).

65. If focus group testing is to occur, it is expected to be undertaken around April 2014.

[redacted]

67. The Census Program plan to return to ELG in mid 2014, after the conduct of testing to recommend a position on the retention of names and addresses for the 2016 Census, and any related policy or procedural changes for the ABS.

[redacted]

[redacted]

Attachment 1 - Recent papers and discussions relevant to the retention of personal identifiers across ABS

In August, the following paper was presented to the Statistical Spatial Framework Steering Committee (Retention of PII for SSFSC _final.docx). The paper sought to promote discussion by the Statistical Spatial Framework Steering Committee (SSFSC) towards forming an agreed position on the retention of personal identifier information by the ABS, highlighting the associated opportunities and risks and proposing a way forward.

Also in August, a paper was presented to the PLASS Survey Managers Committee (see Notes Link) which sought to start discussions and encourage thinking about how to enable PLaSS statistical collections for potential future data integration, and identifying issues that may need to be considered or resolved. In this context, the respective project boards for the General Social Survey (GSS) and the Survey of Disability, Ageing and Carers (SDAC) requested that their collections were set up in such a way as to enable potential use in data integration projects (see Notes Link for GSS example).

Attachment 2 - International approaches to personal identifier retention

It is also worth comparing the ABS position on personal identifiers with that of some of our international counterparts, where there are similar social/public values and similar statistical systems.

In Statistics New Zealand and Statistics Canada, personal information is retained for statistical purposes. In the Office for National Statistics, personal identifiers are converted to anonymous, but unique, codes (referred to as 'pseudo-identifiers'). In all cases, the personal identifiers are securely stored separate from the the data files. The US Bureau of the Census does not retain personal identifiers (from the Census or American Community Survey) outside of the processing period.

Item no. 2 – Minutes of the discussion/decision by ELG regarding Item 1.

ELG/2015/22	Database: **ABS Corporate Information** **Executive Leadership Group** **Summary of outcomes - ELG meeting of 19 October 2015** Author Area: **Office of the Statistician**	**19 Oct 2015**

EXECUTIVE LEADERSHIP GROUP - Summary Outcomes

Purpose of Meeting	**EXECUTIVE LEADERSHIP GROUP (ELG)**
Date	**Monday 19 October 2015**
Chairperson	David Kalisch
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

	Agenda item
1	**Retention of names and addresses in the ABS** [redacted] brought back a paper on ABS retention of names and address in response to request from ELG in late 2013. [redacted] For Census, the paper outlined a number of options for the retention of name and address. ELG agreed to further consider a proposal that retained name and address, but permanently kept name and address separate from the Census data file after the end of Census processing. The name and address could be used for data linkage purposes, but only anonymised name in any linkage processes. ELG agreed to commission a Privacy Impact Assessment (PIA) on the retention of names and addresses for the 2016 Census. The PIA is to be finalised before the end of 2015. The consultation process will involve key stakeholders, including the privacy commissioners and a public notice around intent to conduct an PIA. [redacted] 1-1 [redacted] and Census to work with [redacted] and the Strategic Partnerships and Projects Division to conduct a Privacy Impact Assessment around retention of names and addresses from the 2016 Census.
2	[redacted]

3	**Proposal for a Population and Social Statistics User Group** [redacted] outlined the proposed membership and terms of reference (ToR) for the new cross-cutting Population and Social Statistics User Group. The ToR is based on the Economic Statistics User Group ToR. The Australian Statistician supports the creation of the group but wants membership to target people who will be engaged and add value to the group, and for membership to not be based on department representation. He also requested that states and territories are sufficiently represented. It was agreed that the group should be chaired externally. ELG clarified that the group was an advisory group rather than a user group and the name should reflect the purpose of the group. The ToR also needs to be updated to reflect that this group nor ESUG reports to ASAC. 3-1 [redacted] and DAS SSG to update the name and ToR for the Population and Social Statistics User Group to reflect ELG comments. 3-2 [redacted] and DAS SSG to identify a chair and representatives for the Population and Social Statistics User Group and bring the suggested names back to ELG.
4	**Embargo Policy** [redacted] introduced the draft *Embargo policy* which complements the *Pre-release access policy* already approved by ELG. The *Embargo policy* • enables release at a time other than 11.30am if both the responsible Group Manager and the PM, Communications and Dissemination agree • clarifies that where a publication contains secondary analysis of data from a previously released dataset, it is the analysis, not the data, which is under embargo • allows additional material (such as tailored material) associated with a release to be distributed immediately after the embargo is lifted provided it only shares information contained in the release • requires additional material containing data or analysis not in the release to be withheld for an hour and a half after the release, as it is now. The Australian Statistician outlined the need for a separate category of releases in the policy for which different embargo arrangements may be required. This category should include releases on the processes of the ABS. In some cases the embargo for these is not set by the ABS, such as the release date and time of the Annual Report, which is set by Parliament. The Forward Work Program, the ABS-commissioned Community Trust Survey, the Corporate Plan, the Engagement Strategy, and the Statement of Intent are other examples which should fall in this category. [redacted] was authorised to give final clearance to the *Embargo policy* on behalf of ELG after Governance and Parliamentary Liaison Branch had updated the policy accordingly. 4-1 Governance and Parliamentary Liaison Branch to update the *Embargo policy* to reflect the additional category of releases.
5	[redacted]

	[redacted]
6	**Senate Estimates** Senate Estimates briefing to be held separately.
7	**Communications report** [redacted] outlined that the Community Trust Survey results will be released at 6am to coincide with World Statistics Day (Tuesday 20 October). A joint media release with the Assistant Minister to the Treasurer will be released. An SES Town Hall and the first ABS Transformation Showcase will also occur on World Statistics Day followed by afternoon teas hosted by SES. There will be invited externals to the Transformation Showcase. A Transformation toolkit is being prepared for use in stakeholder engagement with internal and external audiences.

Item no. 3 – Paper to the ABS Executive Leadership Group (ELG) meeting of 8 December 2015 – ‘Outcome of Privacy Impact Assessment: Proposal to retain names and addresses from responses to the 2016 Census’.

Executive Leadership Group

Outcome of Privacy Impact Assessment: Proposal to retain names and addresses from responses to the 2016 Census

Census Program and Strategic Partnerships and Projects Division

Presenter: [redacted]

Observers: [redacted]

8 December 2015

Purpose

To advise ELG members on the outcome of the Privacy Impact Assessment (PIA) on the proposal to retain names and addresses from responses to the 2016 Census.

Key Background

1. ELG agreed on 19 October 2015 to conduct a Privacy Impact Assessment (PIA) on the retention of names and addresses from responses to the 2016.

2. A Media Release and Statement of Intent were published on the ABS website on 17 November 2015. A public feedback period was open for 3 weeks and closed on 2 December 2015.

3. A PIA was undertaken by the Strategic Partnerships and Projects Division, in consultation with the following Divisions: Census and Statistical Network Services Division; the Governance, People and Culture Division; and Technology Services Division.

4. The following key stakeholders have been advised / consulted: ASAC, the AMT and Treasurer's office, the Commonwealth Privacy Commissioner and State/Territory Privacy Commissioners (or relevant Officers).

5. No substantive issues have been flagged during stakeholder consultations or in undertaking the PIA, although a small number of recommendations have been made to support implementation if the proposal proceeds.

6. A decision on whether to retain names and addresses from responses to the 2016 Census is required to be announced before the end of the year to provide sufficient 'air gap' between the announcement and the conduct of the 2016 Census in August 2016.

Action required by ELG

1. Consider the outcome of the PIA and provide any comments on the recommendations and strategies to address identified risks, and whether these recommendations and strategies are rigorous enough to support a decision to proceed with retention of names and addresses.
2. Based on ELGs decision, a communications strategy is provided for discussion and agreement on next steps.

1. The Statement of Intent and Media Release, released on 11 November initiated a 3 week public feedback period on the proposal to retain names and addresses from the 2016 Census. Only three responses from concerned private citizens have been received.

2. The following key stakeholders have been advised or consulted: ASAC, the AMT and Treasurer's office, the Commonwealth Privacy Commissioner and State/Territory Privacy Commissioners (or relevant Officers). The Australian Privacy Commissioner emphasised the need to clearly articulate the mitigation strategies around identify theft, data security and the prevention of data breaches given heightened public concern in this area. No other substantive issues have been raised. A summary of stakeholder engagement and correspondence is provided at Attachment A.

3. Media coverage on the proposal to retain names and addresses from responses to the 2016 Census has consisted of two articles appearing in APS News and IT News. Both articles repackaged material in the Statement of Intent and Media Release.

4. The Strategic Partnerships and Projects Division have completed a PIA on the proposal to retain names and addresses from responses to the 2016 Census (see Attachment B for the PIA and Attachment C for the Outcome of the PIA). The following internal stakeholders have been consulted:
    a. 2016 Census program
    b. ABS Centre for Data Integration
    c. IT & Protective Security
    d. Geospatial Solutions
    e. Policy, Legislation and Assurance
    f. Communications and Dissemination

5. The outcome of the PIA has confirmed that the proposal to retain names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles (APPs).

6. In relation to the proposed retention of names and addresses from responses to the 2016 Census, a small number of potential risks to personal privacy, data security and public perception have been identified. However, the assessment concludes that in each case, the likelihood of the risks eventuating is 'very low'. It also concludes that the ABS has implemented robust processes to manage data, protect privacy and guard against misuse of information, and that these arrangements effectively mitigate these risks. It is judged that any residual risks are such that the ABS is capable of managing.

7. The General Managers of the: Strategic Partnerships and Projects Division; Census and Statistical Network Services; Governance, People and Culture Division, as well as the Program Managers for 2016 Census and Data Integration, met on 4 December to discuss the outcomes of the PIA and public consultation process. The discussion provided feedback to finalise the PIA, recommendations and supporting documents. The group also discussed a range of scenarios, including if a decision to retain names and addresses was not well received from the community and was impacting / likely to impact Census responses. It was noted that any decision to retain names and addressed could be reversed from an operational perspective at any time but that any reversal of the decision would probably have already impacted the trust of some respondents and the subsequent quality of responses to the Census.

8. If a decision is made to retain names and addresses, the following implementation actions are recommended

    a. Update the Census Privacy Statement prior to conducting the Census on 6 August 2016 to ensure transparency by informing the Australian public that names and addresses from responses to the 2016 Census will be retained by the ABS for statistical and operational purposes as long as there is a purpose for doing so. **[Responsibility: Program Manager, 2016 Census]**

    b. Implement business processes which are necessary to manage the separation and retention of names and addresses from responses to the 2016 Census, including separating the internal ownership and responsibility for managing the name file from the area managing the file of anonymised names, and implementing an audit process for Directors responsible for granting access to retained data files.

    [Responsibility: Program Manager, Data Integration and Microdata Futures]

    c. Develop training and support materials for staff accessing name and address data, as well as guidelines for ABS Census Interviewers and publish online responses to frequently asked questions concerning the retention of names and addresses from responses to the 2016 Census to support queries from the public. **[Responsibility: Program Manager, 2016 Census]**

    d. Conduct an internal audit of the implementation of the above recommendations as part of the internal audit program scheduled for the 2017-2018 financial year. **[Responsibility: Program Manager, 2016 Census]**

    e. Assign responsibility to the Senior Executive Committee responsible for approving data integration projects and for monitoring whether there is an ongoing need for the retention of information.
    [Responsibility: Program Manager, Data Integration and Microdata Futures]

9. To communicate the outcome of the PIA, an ABS Minute will be sent to the Assistant Minister to the Treasurer (AMT) on the Australian Statistician's decision (Attachment D). After the AMT has noted this advice, letters will be sent to Commonwealth, State and Territory Privacy Commissioners or equivalent. A Media Release, a statement on the outcome of the PIA, the full PIA and the Executive Summary from focus group testing will be published on the ABS website (See Attachment E for draft Media Release). A NewsPoint will be published, with an advance copy provided to all SES and Census Directors.

10. All further responsibility for communication will be carried out by the Census program. Any feedback or media commentary received after release of the Media Release and PIA will be reviewed and acted upon appropriately by Corporate Communications and the 2016 Census program.

[redacted]
General Manager, Strategic Partnerships and Projects Division
December 2015

Attachment A: Summary of stakeholder engagement and correspondence

Stakeholder engagement	
Minute to the Assistant Minister to the Treasurer, **The Hon Alex Hawke MP**	Sent with follow up discussion with Office. Minute was noted. Updates provided in Weekly Circular
Letters to Commonwealth, State and Territory Information & Privacy Commissioners	David Kalisch called Timothy Pilgrim, Australian Privacy Commissioner [redacted] met with OAIC Advisers to review PIA [redacted] met with Timothy Pilgrim on outcomes of PIA and received additional advice on inclusions for the PIA which have been incorporated. WA, NSW and Victoria responded but did not raise substantive issues.
ASAC advised at scheduled ASAC meeting	Discussion held at ASAC
Other key stakeholders advised: **PM&C, Treasury**	Contacted by [redacted] and Treasury through AMT Minute
Economic Statistics Advisory Group	[redacted] presentation
Census workshops around States/Territories with key Census stakeholders	Feedback noted by Census and PIA team
Consult internally – Census, Policy and Legislation, Security, Geography, SPPD	Preparation of draft privacy risk assessment & recommendations.

Correspondence received	
Sven Bluemmel **Office of the Information Commissioner, WA**	No concerns raised
David Watts **Commissioner for Privacy and Data Protection, Vic**	Request for further detail Responded to by [redacted]
Dr Elizabeth Coombs **NSW Privacy Commissioner**	Request for a copy of the PIA, provided advanced draft. Responded to by [redacted]
Three letters from private citizens	Proposal was not supported
Department of Immigration and Border Protection	Currently with SES of DIBP, not yet received
Department of Social Security	Currently with SES of DSS, not yet received

Attachment B: Privacy Impact Assessment

Australian Bureau of Statistics

Canberra Office
ABS House
45 Benjamin Way
Belconnen ACT 2617
Phone 1300 135 070

Locked Bag 10
Belconnen ACT 2616

www.abs.gov.au
ABN 26 331 428 522

Privacy Impact Assessment:

Proposal to Retain Name and Address Information from Responses to the 2016 Census of Population and Housing

Draft as at: 7 December 2015

Contents

Executive Summary 7

1. Introduction 8

1.1. Project Overview 8

1.2. Privacy Impact Assessment Methodology 8

2. Project Description 9

2.1. Background and Rationale 9

2.2. Legal Authority 10

2.3. Governance and Institutional Arrangements 11

2.4. Retention and Use of Information 13

2.5. Information Flows 14

2.6. Security of Information 18

2.7. Disclosure of Information 20

2.8. Access to and Correction of Information 20

3. Stakeholder Consultation 21

3.1. Overview of Stakeholder Consultation 21

3.2. Outcomes of Stakeholder Consultation 21

4. Privacy Risk and Mitigation 22

4.1. RISK: Unauthorised access to data stored in the ABS environment by ABS staff member 22

4.2. RISK: Unauthorised external access to data stored in the ABS environment 22

4.3. RISK: Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation 23

4.4. RISK: Reduction in public trust in the ABS due to privacy concerns 24

4.5. RISK: 'Function creep' – unintentional expanded future use of retained name and address information 25

5. Conclusion 26

Recommendations 26

Appendix A – Media Release ..... **Error! Bookmark not defined.**

Appendix B – Statement of Intent ..... **Error! Bookmark not defined.**

Executive Summary

The Census of Population and Housing (Census) collects information relating to each person and household in Australia. While the Census collects information relating to each person and household, it is not concerned with information about individuals as such. The Census is taken to provide information about the community as a whole and about groups within the community. The public expects that the information they provide to the ABS will be kept confidential.

The retention of names and addresses from responses to the 2016 Census is a key enabler for improved household surveys and high quality statistics, and ABS' ability to provide a richer and dynamic statistical picture of Australia through the integration of Census data with other survey and administrative data. Names and addresses would be stored separately from other household and person data collected in the Census. Addresses and anonymised versions of names would only be used for projects approved by a Senior Executive Committee, and only if subject to strict security provisions.

The ABS is committed to maintaining the highest levels of community trust and meeting its legislative obligations. No information is or will be released in a way that would enable users of Census data to identify any particular individual or household. Names and addresses would not be passed to another government department or any other organisation.

Consistent with best practice, the ABS has undertaken this Privacy Impact Assessment to identify the risks that the retention of names and addresses from responses to the 2016 Census might have to the privacy of individuals, and to assess the ABS' proposed approach to managing, minimising or eliminating those risks. The Privacy Impact Assessment has been undertaken in accordance with the framework for Privacy Impact Assessments set out in the Office of the Australian Information Commissioner's *Guide to undertaking Privacy Impact Assessments*. The ABS also referred to the Office of the Australian Information Commissioner's *Guide to information security* and *Guide to handling personal information security breaches*.

The outcome of the Privacy Impact Assessment has determined that the retention of names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

The Privacy Impact Assessment identified a small number of potential risks to personal privacy associated with the retention of names and addresses from responses to the 2016 Census, but concluded that in each case the likelihood of these risks eventuating was 'very low'. The Privacy Impact Assessment determined that these risks can and will be effectively mitigated by implementation of a functional separation principle and by existing governance and security arrangements in place in the ABS. A small number of recommendations have been made in relation to implementation of the proposal.

The outcome of this Privacy Impact Assessment, along with feedback from key stakeholders and the public, will inform the ABS' decision to retain names and addresses from responses to the 2016 Census. The ABS will publish its decision and this Privacy Impact Assessment on the ABS website by the end of the year.

1. Introduction

1.1. Project Overview

The Australian Bureau of Statistics (ABS) is conducting this Privacy Impact Assessment on the retention of names and addresses from responses to the 2016 Census of Population and Housing (Census).

Historically, the ABS has destroyed name and address information after statistical processing of the Census has been completed.[1] The ABS is now considering the retention of names and addresses from the 2016 Census as a key enabler for improved household surveys and high quality statistics, and to support the integration of Census data with other survey and administrative data to provide a richer and dynamic statistical picture of Australia.

In considering this change, the ABS remains committed to maintaining the highest levels of community trust and meeting its legislative obligations. The proposal to retain names and addresses from responses to the Census is made in accordance with the provisions for protecting personal privacy in the *Census and Statistics Act 1905* (Cth) and the *Privacy Act 1988* (Cth), including the Australian Privacy Principles. No information will be released by the ABS in a way that would enable users of Census data to identify any particular individual or household.

The proposal is for names and addresses to be stored separately from other household and person data collected in the Census. It is also proposed that addresses and anonymised versions of names will only be used for approved projects subject to strict security provisions.

To inform the ABS' decision and approach, the ABS has undertaken this Privacy Impact Assessment and has sought feedback on this proposal. A Media Release and Statement of Intent were released by the ABS on 11 November 2015. Feedback on the proposal was sought by 2 December 2015. Stakeholder feedback has been considered in finalising this Assessment.

1.2. Privacy Impact Assessment Methodology

Australian Privacy Principle 1 requires Australian Privacy Principle entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the Australian Privacy Principles and enable them to deal with enquiries or complaints about privacy compliance. In this way, the Australian Privacy Principles require 'privacy by design', an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards.

As detailed below, the ABS has established governance systems consistent with Australian Privacy Principle 1. In the interests of transparency, the ABS has undertaken this Privacy Impact Assessment to identify the risks that the proposal to retain names and addresses from responses to the Census

[1] Currently, the ABS destroys all name-identified Census information after statistical processing except where people have explicitly consented to their personal information being retained for 99 years by the National Archives of Australia as part of the Census Time Capsule. The ABS proposal to retain name and address information from responses to the 2016 Census is independent of the Census Time Capsule scheme.

might have on the privacy of individuals, and to assess the ABS' proposed approach to managing, minimising or eliminating those risks. This Privacy Impact Assessment has been undertaken in accordance with the framework for Privacy Impact Assessments set out in the Office of the Australian Information Commissioner's *Guide to undertaking Privacy Impact Assessments*.[2] The ABS has also referred to Office of the Australian Information Commissioner's *Guide to information security*[3] and *Guide to handling personal information security breaches*[4].

As a part of the decision making process on whether to adopt the proposal, feedback has been sought directly from Commonwealth, State and Territory Information and/or Privacy Commissioners, or relevant representatives. Feedback has also been sought from the public via a media release and Statement of Intent published on the ABS website. See Appendix A for the Media Release and Appendix B for the Statement of Intent.

The ABS will review the outcomes of this Privacy Impact Assessment and take into consideration all feedback received to enable an informed decision to be made on whether to proceed with the proposal to retain names and address from responses to the 2016 Census.

2. Project Description

2.1. Background and Rationale

Australia's seventeenth national Census will be held on Tuesday, 9 August 2016. The Census provides a comprehensive picture of Australians in order to inform decision-making, policy development, and the provision of funding and services by governments and other users.

The ABS has four goals for the 2016 Census. These are to:

1. count every dwelling and person in Australia on Census night;
2. maximise the value of Census data to all users;
3. protect the privacy of the public; and
4. increase the efficiency and sustainability of the Census.

Consistent with these goals, the 2016 Census will be a launching pad for a transformation of the way the ABS collects and provides access to data about Australia's population. The ABS aims to move to an integrated approach to the collection and compilation of data from existing datasets. The 2016 Census will also provide an opportunity to improve and expand the information available to Australians through continuing the use of statistical data integration techniques to bring together 2016 Census data with previous Censuses (2006 and 2011) and other survey and administrative datasets. Together these initiatives will continue to provide new analytical insights and ensure that the Census delivers maximum benefit to governments and the community.

---

[2] Office of the Australian Information Commissioner (May 2014), *Guide to undertaking privacy impact assessments.*
[3] Office of the Australian Information Commissioner (August 2014), *Guide to information security*.
[4] Office of the Australian Information Commissioner (August 2014), *Guide to handling personal information security breaches*.

As part of this transformation, the ABS is exploring the retention of names and addresses from responses to the 2016 Census to provide a benefit to the ABS and wider community by:

- enabling higher quality and more efficient linkage of high value survey and administrative datasets with the Census, particularly for small or highly mobile sub-populations of policy interest;
- supporting a range of organisational efficiencies, such as the development of an address register, improving sampling, imputation and provider management; and
- supporting more flexible geospatial outputs.

In considering this proposal, the ABS remains committed to maintaining the highest levels of community trust. The ABS will apply well established separation principles to protect privacy and data by storing both names and addresses separately and securely from other household and personal data collected in the Census. Addresses and anonymised versions of names will only be used for approved projects which are subject to strict security provisions. No information will be released by the ABS in a way that would enable users of Census data to identify any particular individual or household.

This Privacy Impact Assessment ensures that appropriate identification and assessment of risks has been undertaken, and that appropriate controls have been implemented to mitigate the risks. This will ensure the right approach is taken to enable the secure retention of name and address information from responses to the 2016 Census.

A decision on whether to proceed with the proposal to retain name and address information from responses to the 2016 Census, informed by this Privacy Impact Assessment and stakeholder feedback, will be made and the outcome published by the end of 2015.

2.2. Legal Authority

The *Australian Bureau of Statistics Act 1975* (Cth) and the *Census and Statistics Act 1905* (Cth) set out the primary functions, duties and powers of the ABS. The ABS is also subject to the *Privacy Act 1988* (Cth).

The *Australian Bureau of Statistics Act 1975* establishes the ABS as an independent statutory authority. Section 6 prescribes its functions to include the collection, compilation, analysis and dissemination of statistics and related information.

The *Census and Statistics Act 1905*:

- empowers the Australian Statistician to collect statistical information on a broad range of demographic, economic, environmental and social topics;
- enables the Australian Statistician to direct a person to provide statistical information, in which case they are legally obliged to do so;
- requires the ABS to publish the results of these statistical collections;
- places a life-long obligation on all ABS officers to maintain the secrecy of information collected under the Act, and provides harsh penalties for those who fail to do so; and

- does not allow data to be published in a manner that is likely to enable the identification of a particular person or organisation.

The ABS undertakes the Census every five years in accordance with the *Census and Statistics Act 1905*. Names and addresses are among the matters in relation to which the Statistician may collect information, as prescribed by regulation 6 and Schedule 1 of the *Census and Statistics (Census) Regulations 2005* (Cth).

The proposal to permanently retain name and address information from responses to the 2016 Census does not involve the collection of additional information than that collected in the 2011 Census.

The *Census and Statistics Act 1905* requires the ABS to publish results in a manner not likely to identify a particular person, household or organisation. Section 19 of the *Census and Statistics Act 1905* forbids past or present officers of the ABS (which includes temporary staff) from divulging information collected under this Act, either directly or indirectly, under penalty of up to 120 penalty units (currently $21,600) or imprisonment for two years, or both. To ensure that confidentiality and privacy provisions are observed, all officers of the ABS sign legally binding undertakings to comply with the secrecy provisions of the *Census and Statistics Act 1905*. These undertakings are binding for life and are renewed annually.

The ABS also has an obligation to comply with the *Privacy Act 1988*, including the Australian Privacy Principles. The Australian Privacy Principles regulate how the ABS may collect, use, disclose and store personal information. In accordance with Australian Privacy Principle 3, the ABS may collect personal information (such as name and address) where it is reasonably necessary for, or directly related to, its functions or activities. Australian Privacy Principle 11 provides that the ABS may retain the personal information of an individual where that information continues to meet a business need that is aligned with the purpose for which the information was collected.

The proposal to retain names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

2.3. Governance and Institutional Arrangements

The ABS is Australia's national statistical agency, providing trusted official statistics on a wide range of economic, social, population and environmental matters of importance to Australia. A recent independent survey showed that trust in the ABS remains high and that 81 per cent of the general public and 100 per cent of informed users trust Australia's official statistical organisation, the ABS.

The ABS and its staff uphold the Australian Public Service (APS) Values and Code of Conduct. These values, which are congruent to the ABS's role as an independent provider of statistical information for Australia, are summarised in the following table:

Impartial	The APS is apolitical and provides the Government with advice that is frank, honest, timely and based on the best available evidence.
Committed to Service	The APS is professional, objective, innovative and efficient, and works collaboratively to achieve the best results for the Australian community and the Government.
Accountable	The APS is open and accountable to the Australian community under the law and within the framework of Ministerial responsibility.
Respectful	The APS respects all people, including their rights and their heritage.
Ethical	The APS demonstrates leadership, is trustworthy, and acts with integrity, in all that it does.

The ABS has a long history of, and a strong culture for, protecting the privacy of individuals and the confidentiality of information supplied by them. The protection of privacy is considered paramount to the successful conduct of the Census. The ABS maintains a Privacy Policy which sets out its personal information handling practices. The ABS Privacy Policy can be found at www.abs.gov.au/privacy. The Census Privacy Statement will be released before August 2016 and will be found at www.abs.gov.au/census.

In 2012, the ABS became an accredited Integrating Authority under the Commonwealth statistical data integration interim arrangements. Statistical data integration involves combining data from different sources to provide enhanced datasets for statistical and research purposes – which excludes purposes such as delivery of services to particular individuals, individual compliance monitoring, client management, incident investigation, or regulatory purposes.

As an accredited Integrating Authority, the ABS has been authorised as a safe and effective environment for data integration projects involving Commonwealth data. The ABS was accredited against the following criteria:

- ability to ensure secure data management;
- information that is likely to enable identification of individuals or organisations is not disclosed to external users;
- availability of appropriate skills;
- appropriate technical capability;
- lack of conflict of interest;
- culture and values that ensure protection of confidential information and support the use of data as a strategic resource;
- transparency of operation; and
- existence of an appropriate governance and institutional framework.

A copy of the accreditation claims made by ABS, which have been verified by an independent auditor, is available through the National Statistical Service website.

Consistent with its accreditation status, the ABS has well-established governance infrastructure and procedures to manage the approval, conduct and review of statistical data integration projects

undertaken by the ABS. A Senior Committee comprised of senior level ABS staff (SES Band 2 / SES Band 1 level) oversees this process. All data integration projects undertaken by the ABS must be approved by the Committee prior to integration commencing. Approval is based on a written application endorsed by the project owner (SES Band 1 level) which covers the proposed data and risk management strategies for the project. Projects which the Committee deem to be 'high risk' under the Commonwealth Data Integration Risk Assessment Guidelines require approval by the Australian Statistician. Project owners must notify the Committee of any proposed amendments to their project, and if a major amendment is needed, submit a new proposal for approval. In the interests of transparency, outlines of approved data integration projects within scope of the Commonwealth arrangements are published on the ABS website.

2.4. Retention and Use of Information

The Census collects information relating to each person and household in Australia. While the Census collects information relating to each person and household in the country, it is not concerned with information about individuals as such. The Census is taken to provide information about the community as a whole and about groups within the community. The public expects that the information they provide will be kept confidential.

Protection of personal privacy is paramount at the ABS. Based on a strong track record, people can be confident that the ABS will keep their personal information secure – both that provided on paper Census forms and the online eCensus. The ABS has never released such information to any outside organisation, agency or project consistent with the legal requirements described in Section 2.2.

The ABS proposes to retain names and addresses from responses to the 2016 Census for statistical and operational purposes within the existing protective legislative and procedural frameworks, with no disclosure of identifiable personal information.

Consistent with Australian Privacy Principle 11, name and address information will only be retained where there continues to be a business need for doing so. After processing of the Census data, names and addresses will be separated from other personal and household information on the Census data set. Names will not be brought back together with other information collected from respondents to the Census. Anonymised versions of names will be generated for data integration purposes and addresses geocoded.

This Privacy Impact Assessment will inform the decision on whether the ABS will retain the names and addresses collected from responses to the Census; the outcome of this decision will be published by the end of 2015. If a decision is made to proceed with the proposal, the ABS will ensure transparency of this decision and how personal information will be managed, consistent with Australian Privacy Principle 1. It will do this by:

1. publishing the decision and the privacy impact assessment on the ABS website by the end of the year;
2. detailing how Census name and address information will be held and used by the ABS in the publication – 'How Australia takes a Census', to be published in March 2016;
3. releasing the Census Privacy Statement before the 2016 Census; and

4. publishing responses to frequently asked questions for participants of the Census.

2.5. Information Flows

Following the completion of Census processing, the ABS proposes to permanently separate name and address information from other information on the Census dataset, and to store names and addresses separately and securely. This is considered a key element of the privacy design, protecting against the accidental or malicious disclosure of personal information from responses to the 2016 Census.

The separation principle will be enforced to separate name and address variables from analysis or content information during both data storage and use in statistical data integration or for operational purposes. The separation principle is a well-established approach applied internationally to protect privacy and the security of data by ensuring that no one working with the data can view both identifying information (such as name and address) together with the analysis or content data (such as tenure type or educational attainment). As an accredited Integrating Authority, the ABS has been audited and accredited for its application of the separation principle for the purposes of statistical data integration activities.

Under the separation principle, authorised ABS officers will only have access to the information required to support their role. This means that only a limited number of ABS staff will have access to the retained information.

The key layers of protection that will be in place as a result of applying functional separation are:

- names, anonymised names, addresses and other Census information will be stored separately;
- no individuals will have access to both names and other Census information;
- no individual will have the ability to grant themselves access to any data files;
- individuals who undertake linkage of data sets (using anonymised name) will not undertake the analysis of the data;
- individuals with access to data files will be reviewed monthly.

The proposed functional separation roles as applied for data integration projects are outlined in Box 1.

Box 1. Functional Separation Roles

Functional separation involves placing project members into separate roles during the lifecycle of a data integration project. Access to data will vary depending on the role that each project member performs. Under the separation principle, any one project member is prevented from accessing both identifying and analytical information from datasets during the linkage process.

There are four roles, as follows, of which the first two are most relevant to the proposal:

Librarian: A staff member in this role performs processes such as the acquisition of data to be used for linking purposes, standardisation of the data and creation of the files for input into linking. Separation is maintained by staff only performing one role at a time per project. Librarians may also be responsible for creating anonymised linkage keys for names for additional or new datasets such as survey and administrative data. These anonymised keys will be stored separately to the file containing names.

Linker: A staff member in this role performs the linkage of the two datasets. Their access is limited to fields they require for linking and clerical review (when applicable), which can include identifying information such as anonymised name and address.

Assembler: A staff member in this role takes the linked outputs (from the linker) and combines them with the analysis variables provided by the data custodian. At this point a new identifier, 'Analysis identifier', is created for research and analysis to be undertaken.

Analyst: A researcher in this role performs analysis on the linked dataset. Their access is limited to data needed for analytical purposes, which typically does not include identifying information.

Staff in the above roles will be provided with access to data on a need-to-know basis by a designated Role Manager, with access restricted to either the linking or the analysis information based on their data requirements.

The process flows for the retention of names and addresses from responses to the 2016 Census are outlined below.

Name Information

Once processing is complete, names will be separated from the remainder of the Census dataset, and retained in a separate file as long as there is a purpose for doing so (consistent with Australian Privacy Principle 11). Names will not be brought back together with other information collected from respondents to the Census. Anonymised versions of names will be generated from the names and stored separately from both the file of names and the Census dataset. The name and anonymised name files will be the responsibility of functionally separate sections in the ABS.

Access to and use of the name file will be restricted and subject to approval from the Program Manager, Data Integration and Microdata Futures (SES Band 1) in order to create new anonymised versions of names to ensure linkage keys for statistical data integration keep pace with evolving standards and methodology and are fit-for-purpose.

The anonymised name file will be used as a resource for data linkage research and practice, forming part of the foundational infrastructure underpinning statistical data integration activities involving Census data.

Neither names nor anonymised names will be part of a Census analytical file, nor will this information ever be disclosed by the ABS.

This functional separation approach is consistent with international best practice, and is similar to practices utilised effectively by the Office of National Statistics in the United Kingdom.

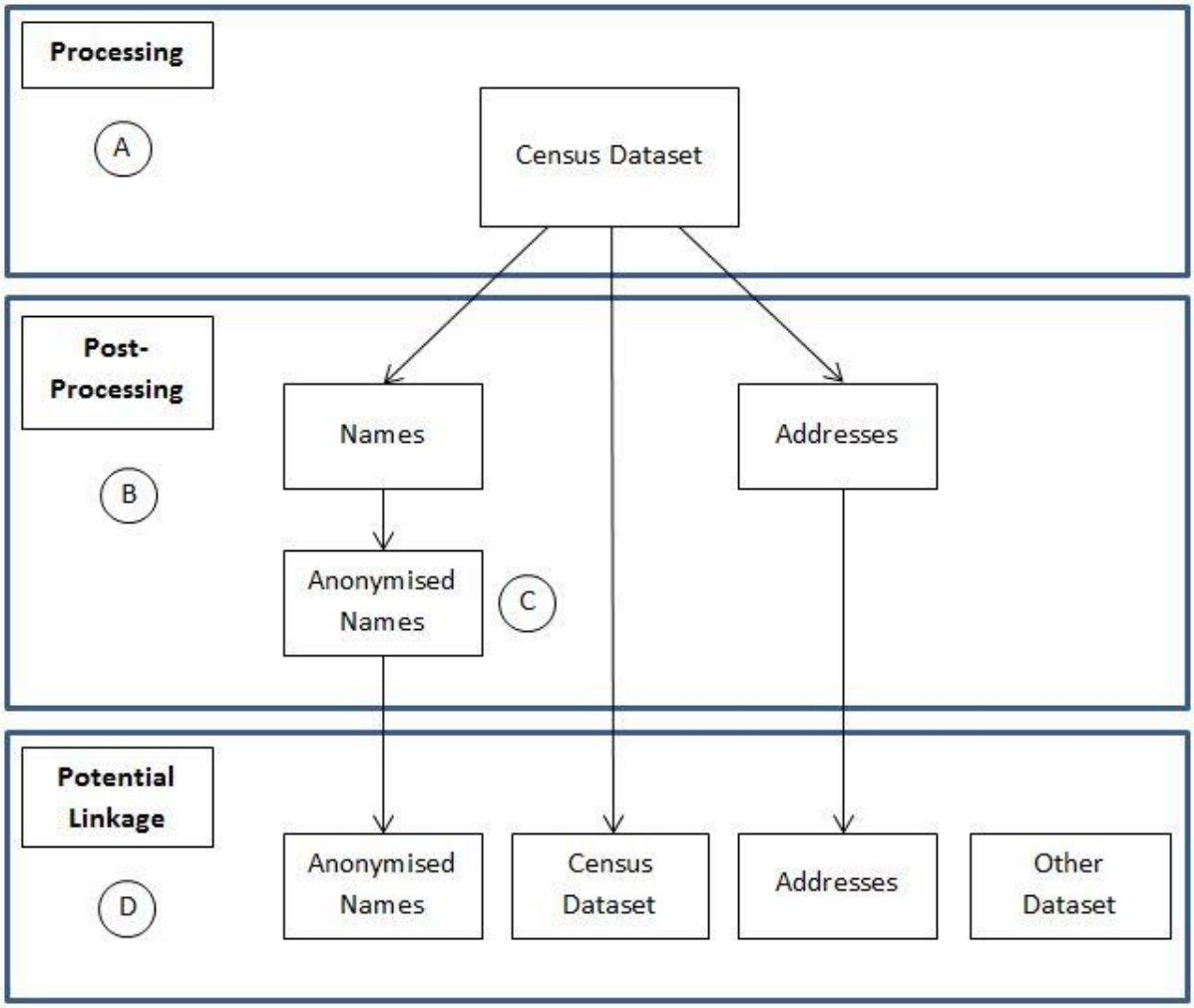
Address Information

Once processing is complete, addresses and their associated coordinate geocodes will be retained separate to the Census dataset as long as there is a purpose for doing so (consistent with Australian Privacy Principle 11). This file will only be for internal use.

Once separated from the Census dataset, addresses will not be brought back together with other personal and household information in the Census dataset. The Director, Geospatial Solutions (Executive Level 2) will have responsibility for the address file, and for approving internal access to the file where there is a demonstrated need to do so.

Address information from the 2016 Census will be used to support the improvement of geospatial statistics, the ABS Address Register, and other operational efficiencies.

Figure 1. Map of Information Flows



A. ABS 2016 Census staff will collect and process data from the 2016 Census.
B. Once processing is complete, names and addresses will be permanently separated from the remainder of the Census dataset, and stored securely in separate files with restricted access.
C. Anonymised versions of names will be generated from the names; these will be stored separately from both the file of names and the Census dataset. ABS staff in the librarian role will perform these functions.
D. For approved data integration projects involving 2016 Census data, staff in the librarian role will recombine demographic and anonymised name information on an as-needed basis to allow the Census dataset to be used for statistical data linkage. ABS staff in the linker role will perform the linking.

2.6. Security of Information

The ABS has an embedded culture of security and compliance, and has established robust and effective processes to protect the integrity and privacy of information collected from individuals and businesses.

The ABS complies with the mandatory requirements established by the Australian Commonwealth *Protective Security Policy Framework* (PSPF). The PSPF provides the appropriate controls for the Australian Government to protect its people, information and assets, at home and overseas.

The ABS also takes reasonable steps to comply with the Office of the Australian Information Commissioner *Guide to information security*[5] and *Guide to handling personal information security breaches*[6].

Governance Security

To enhance physical, IT and systems security, the ABS has established governance arrangements including reporting to the portfolio Minister (the Treasurer) on compliance with the PSPF, implementing risk management policies and strategies, and creating and maintaining security plans.

The ABS has a rolling annual audit program, including audits of protective security (which focusses on different areas such as building access, document handling and contractors), information security and access (which focusses on different systems such as secure deposit box, email, computer assisted interviewing, and laptops). These audits are undertaken annually.

Personnel and Physical Security

All ABS staff and contractors who require unescorted access to ABS premises are required to undergo a pre-employment suitability and eligibility assessment. This requirement may be waived in certain circumstances, such as confirmation from the vetting authority that the person has recently obtained a National Security clearance. They will also undergo police checks and be required to make a declaration of interests to ensure there are no conflicts of interest prior to employment commencing.

Access to ABS physical premises, excluding public areas, is at all times restricted to approved persons, and controls such as an electronic access control system, sign-in registers, reception personnel and security guards are in place.

Information Security

The ABS recognises and strongly respects the information security responsibility it bears as a result of retaining names and addresses. People can be confident in the numerous and robust security measures implemented by the ABS to safeguard their data to prevent identity theft or misuse of data.

[5] Office of the Australian Information Commissioner (August 2014), *Guide to information security*.
[6] Office of the Australian Information Commissioner (August 2014), *Guide to handling personal information security breaches*.

The ABS has an excellent track record of data security, with few serious breaches over its history, and is committed to ensuring this position continues into the future. The prosecution and conviction of a former staff member for an economic data breach (not a privacy breach) demonstrates that the ABS and the Australian judicial system has no tolerance for malicious acts of data breach and the ABS will not hesitate to apply the full authority of the law to these acts. Such a breach was unprecedented in ABS' 110 year history and resulted in an independent review of security arrangements (The Gibson Review). The outcome of the review was a set of recommendations, all of which were implemented, resulting in greater assurance that sensitive information in the possession of the ABS is more secure and controls on information stores are more robust. The ABS also applies secure practices to avoid accidental breaches.

The ABS information technology environment has comprehensive security measures in place, including the most effective Australian Signal Directorate Strategies to Mitigate Targeted Cyber Intrusions and industry best practice. The ABS was a part of an Australian National Audit Office cross-agency audit in 2014 on information technology system security against cyber attacks. The ABS was rated as being in a Cyber Secure Zone (having high-level protection from external attacks and internal breaches and disclosure of information).[7]

A key protection against identity theft is the 'privacy by design' concept to address personal information security. The ABS is fully compliant with the Australian Government's core security policies (The Protective Security Policy Framework and Information Security Manual) and have designed privacy into the application of whole of government information security through the use of the unique Dissemination Limiting Marker) "Sensitive: Statistics" for any information collected under the C&S Act. As a result, email servers and gateway security have been configured to block emails with this Dissemination Limiting Marker, and this in turn reduces the likelihood of accidental data leakage via digital means.

The current information security practices that are in place within the ABS to safeguard data include:

1. high level encryption of data, including tight security around the storage and creation of the encryption keys;
2. an audited linking environment, involving staff activity being logged, monitored and, if inappropriate activity is found, investigated. Any misuse will result in immediate termination of access for the staff member, with further sanctions imposed if necessary;
3. ABS staff and in-posted officers sign legally binding Undertakings of Fidelity and Secrecy to ensure they are aware of their obligation to protect confidential information, and the consequences of disclosure (which include criminal penalties);
4. enforce the clear desks and clear screen policy;
5. access on a 'need to know' basis;
6. annual IT audits;
7. Vulnerability Assessments are carried out on all new IT Systems by specialised staff in IT Security trained in the field of Ethical Hacking;
8. ethical hacks carried out every 12 months on existing systems;
9. Protective Security Management Committee reviewing security risks quarterly;

[7] *Cyber Attacks: Securing Agencies' ICT Systems*, ANAO Audit Report No.50 2013–14, http://www.anao.gov.au/Publications/Audit-Reports/2013-2014/Cyber-Attacks-Securing-Agencies-ICT-Systems/Audit-summary

10. ongoing and reporting of compliance with Government Security Policy including the Protective Security Policy Framework and Australian Signal's Directorate Information Security Manual.

The additional information security practices that the ABS will implement, as a result of retaining names and addresses, are the following:

1. restricted access to the separated name and address files. Within the linking environment, access is further restricted based on staff roles, for instance individuals who undertake linkage of data sets (using anonymised name) will not undertake the analysis of the linked data;
2. ongoing audit of IT access and review of staff who have access to retained information to ensure only necessary persons are included and make regular review of those lists an office-wide priority for management;
3. require the Director responsible for the data to certify that the access lists are correct and if not, who should be removed;
4. provision of additional education and support to staff to ensure adherence to responsibilities of retained name and address details;
5. prevent unauthorised staff from physically entering specialist areas when there are information access restrictions in place;
6. establish procedures to enable ready determination by the relevant officers of all persons who have authority to view specified sensitive information at any point in time.

These combined measures will safeguard retained name and address information and address confidentiality, privacy, identify theft and security risks.

2.7. Disclosure of Information

In accordance with the *Census and Statistics Act 1905*, name and address information from the 2016 Census, as well as outputs from any secondary integrated datasets using Census data, will not be disclosed, published or disseminated in a manner which is likely to enable the identification of a particular person, household or organisation.

Section 19 of the *Census and Statistics Act 1905* makes it an offence for any past or present ABS officer to divulge, either directly or indirectly, any confidential information collected under this Act. The Act provides for heavy criminal penalties (fines of up to $21,600 or imprisonment for 2 years or both) for anybody convicted of breaching this obligation - even if they are no longer employed by the ABS. Staff are required to sign Undertakings of Fidelity and Secrecy which are renewed annually.

2.8. Access to and Correction of Information

In accordance with Australian Privacy Principles 12 and 13, respondents have the right to request access to their personal information held by the ABS and to request its correction. This is clearly stated in the ABS Privacy Policy, which is publically available on the ABS website. If such a request is made, the ABS will respond within 30 days. No charge is made to individuals for requesting access to or correction of their information, or for access being granted.

A decision by the ABS to grant a privacy request to access or correct an individual's personal information will take into account whether the ABS is required or authorised to refuse the request under relevant legislation including the *Freedom of Information Act 1982* or any other Commonwealth legislation which provides for access by persons to documents, in particular the *Census and Statistics Act 1905.*

The ABS Privacy Policy provides information and contact details for individuals who are concerned that the ABS may have breached its responsibilities or their privacy rights. The ABS acknowledges complaints within five business days of receipt, and will investigate and respond within 30 days for non-complex matters.

3. Stakeholder Consultation

3.1. Overview of Stakeholder Consultation

The ABS sought public submissions on both the nature and content of the 2016 Census from November 2012 to May 2013. In August 2015, the ABS published and promoted the 'Census of Population & Housing: Nature and Content, Australia, 2016' which highlighted that the ABS is considering the retention of both names and addresses for statistical purposes. In October 2015, the ABS published the 'Information Paper: Census of Population and Housing – Proposed Products and Services, 2016' which highlighted that data integration will continue to be a central element of the Census.

In November 2015, the ABS directly notified key internal and external stakeholders of its proposal to retain names and addresses from responses to the 2016 Census, and invited feedback to inform this Privacy Impact Assessment and the final decision on whether to adopt the proposal.

The ABS publicised its intent to conduct a Privacy Impact Assessment by publishing a Statement of Intent on the ABS website in November 2015, as well as a Media Release directing attention to the Statement of Intent. Both releases included an invitation to comment and provided contact details to facilitate this.

In order to understand modern community expectations, the ABS has conducted a series of focus groups across the country, arranged through a market research company, in order to understand public attitudes and acceptability of the retention of name and address information from the Census. The general feedback of focus groups were supportive of this kind of change, expressing appreciation of the value of high quality data integration and general comfort in the protections that the ABS would put in place to preserve privacy and confidentiality. However, a key element underpinning this feedback was the need for the ABS to be transparent about how it handles people's personal information.

3.2. Outcomes of Stakeholder Consultation

Contact with the Australian Privacy Commissioner, of the Office of the Australian Information Commissioner (OAIC), by the Australian Statistician resulted in further information being requested

by the OAIC office to inform their review of this proposal. Subsequent review by OAIC Advisers, in conjunction with ABS officers, has affirmed that this ABS Privacy Impact Assessment meets regulatory obligations. No substantive concerns were raised by the OAIC. [Statement to be confirmed with OIAC]

Contact with the State and Territory Privacy Commissioners or relevant representatives for each State and Territory on this matter was made via a letter and copy of the Statement of Intent and Media Release. No substantive concerns were raised by these offices.

Public feedback consisted of three responses from private citizens. All responses focussed on concerns around protecting the privacy of their personal details.

Media coverage consisted of two articles of which the nature was informative and favourable. Articles appeared in IT News (12/11/2015) and PS News (13/11/2015).

After consideration of this Privacy Impact Assessment and of all feedback received, the ABS will decide whether to proceed with the proposal to retain names and addresses from responses to the 2016 Census. The outcome of this decision will be published in December 2015, and will be further described in the March 2016 publication of 'How Australia takes a Census' and reflected in the Census Privacy Statement.

4. Privacy Risk and Mitigation

4.1. RISK: Unauthorised access to data stored in the ABS environment by ABS staff member

Likelihood: Very low.

Consequence of breach: ABS staff may inadvertently or maliciously identify an individual.

Management of risk: To guard against identification of an individual, and any subsequent misuse of their personal information, by a staff member, the functional separation principle and security arrangements will be implemented, as detailed in Sections 2.5 and 2.6.

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Notify affected individuals of the breach;
- Implement immediate mitigating controls to prevent further spreading of the breach;
- Involve ABS security, senior line management and possibly the police.

4.2. RISK: Unauthorised external access to data stored in the ABS environment

Likelihood: Very low.

Consequence of breach: The consequences of breach of privacy depend on whether names, anonymised names, or linked data is accessed.

- Data contained in anonymised or linked datasets will only be brought together by anonymised linkage keys and is unlikely to enable direct identification of an individual or household.
- If names or addresses are accessed, individuals or households are likely to be directly identifiable but no other information about the individual would be available.

Management of risk:

- Functional separation principle implemented – see Sections 2.5 and 2.6 for details;
- Access to name and anonymised name is restricted and role based and the data is contained in separate files located in different areas of the ABS;
- names and addresses will never be put back with Census data.
- no individuals will have access to both names and other Census information;
- no individual will have the ability to grant themselves access to any Census data files;
- individuals who undertake linkage of data sets (using anonymised name) will not undertake the analysis of the linked data;
- individuals with access to data files will be reviewed monthly;
- Data is stored in a secure environment in accordance with the mandatory requirements of the Australian Government Protective Security Policy Framework (PSPF) and consistent with the Information and Communications Technology Security Manual (ISM).

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Endeavour to recover the data;
- Implement immediate mitigating controls to prevent further spreading of the breach;
- Notify affected individuals of the breach;
- Involve ABS security and the Australian Federal Police.

4.3. RISK: Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation

Likelihood: Very low.

Consequence of breach: Name and/or address information is released, resulting in a reduction in trust in the ABS.

Management of risk:

The ABS already successfully manages and protects the privacy of Australians throughout data integration processes involving sensitive datasets, including the Census, and thus effective privacy protections are already in place and in practice.

ABS staff are legally obliged to ensure that data will not be released in a manner which is likely to enable the identification of a person. This is a requirement under the *Census and Statistics Act 1905*; under the Act, ABS staff are subject to criminal penalties if found guilty of breaching its secrecy

provisions. Staff sign annual undertakings acknowledging they understand their legal obligations as well as undertake training on the handling of personal information.

The separation principle will be enforced to separate names and addresses from analysis or content information during data storage, linking and analysis. Names and addresses will never be put back with Census data.

Staff who require access to name and address information from the Census for their approved role will only access this information through secure electronic server environments, reducing the risk of an accidental release of personal information through potential loss of IT equipment such as a laptop or work documents (for example emails).

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Endeavour to recover the data;
- Notify affected individuals of the breach;
- Involve ABS security, senior line management and possibly the police.

4.4. RISK: Reduction in public trust in the ABS due to privacy concerns

Likelihood: Very low

Consequence: The proposal to retain names and addresses from responses to the Census may cause public concern which results in a reduction of participation levels in ABS collections, and/or a public backlash.

Management of risk: To mitigate this risk, the ABS:

- Has informed Commonwealth, State and Territory Information and Privacy Commissioners of the proposal and has committed to addressing any feedback;
- Sought feedback from the public through publication of a Media Release and a Statement of Intent;
- Will comply with established legislative and procedural frameworks which safeguard privacy and data security;
- Will be transparent about objectives, processes and outcomes.
- Will prepare responses to Frequently Asked Questions and ensure Census interviewers are equipped to respond to concerns from respondents.

Management if risk eventuates: Depending on the circumstances, the ABS will:

- Respond to concern from the media, stakeholders and the public;
- Conduct further consultations;
- Reconsider the privacy design for the proposal, if required.

4.5. RISK: 'Function creep' – unintentional expanded future use of retained name and address information

Likelihood: Very low

Consequence: In the future, name and address information from responses to the 2016 Census may be used for purposes beyond what is currently contemplated by the ABS.

Management of risk: Compliance with the legislative and governance framework described in Section 2.2 will guard against function creep by ensuring that:

- names and addresses are retained in accordance with the Australian Privacy Principles;
- any data integration project involving retained information is undertaken for statistical and research purposes only;
- no information will be released in a manner which would enable the identification of a person or household.

In addition, usage of name and address information from responses to the 2016 Census will be subject to established approval, evaluation and review procedures including:

- Internal approval processes, as described in Section 2.3, for data integration projects which assesses the benefits and risks of each project and their compliance with ABS policies;
- Periodic reviews of policies including the policy on retention of personal information and the privacy policy, to ensure these policies are achieving their objectives, are implemented in practice, and remain aligned with public commitments made by the ABS;
- Annual internal audits of information and protective (physical) security.

Management if risk eventuates: Depending on the circumstances, the ABS will:

- Consult affected stakeholders;
- Review relevant internal policies.

5. Conclusion

The outcome of this Privacy Impact Assessment has determined that the proposal to retain names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

In relation to the proposed retention of names and addresses from responses to the 2016 Census, a small number of potential risks to personal privacy and public perception have been identified. This assessment concludes that in each case, the likelihood of the risks eventuating is 'very low'. It also concludes that the ABS has implemented robust processes to manage data and protect privacy, and that these arrangements effectively mitigate these risks. Any residual risks are such that the ABS is capable of managing.

Recommendations

In accordance with the above conclusions, it is recommended that the ABS:

1. Retain names and addresses from responses to the 2016.
2. Update the Census Privacy Policy prior to conducting the Census on 9 August 2016 to ensure the Australian public are informed that names and addresses from responses to the 2016 Census will be retained by the ABS for statistical and operational purposes as long as there is a purpose for doing so.
3. Implement business processes which are necessary to manage the separation and retention of names and addresses from responses to the 2016 Census, including separating the internal ownership and responsibility for managing the name file from the area managing the file of anonymised names, and implementing an audit process for Directors responsible for granting access to retained data files.
4. Develop training and support materials for staff accessing name and address data as well as guidelines for ABS Census Interviewers, and publish online responses to frequently asked questions concerning the retention of names and addresses from responses to the 2016 Census to support queries from the public.
5. Conduct an internal audit of the implementation of the above recommendations as part of the internal audit program scheduled for the 2017-2018 financial year.
6. Assign clear responsibility to a Senior Executive Committee for monitoring whether there is an ongoing need for the retention of name and address information.

Attachment C: Outcome of PIA

Outcome of Privacy Impact Assessment: Retention of names and addresses from responses to the 2016 Census of Population and Housing

Introduction

The Census of Population and Housing (Census) provides a comprehensive picture of Australians in order to inform decision-making, policy development, and the provision of funding and services by governments and other sectors. The 2016 Census, scheduled for Tuesday 9 August 2016, will be a launching pad for a transformation of the way the ABS collects and provides access to data about Australia's population.

Historically, the ABS has destroyed name and address information after statistical processing of the Census has been completed. To enable the ABS to provide a richer and dynamic statistical picture of Australia, the ABS is changing this historical practice for the 2016 Census. For the 2016 Census the ABS will retain names and addresses after processing is completed. This change will support higher quality official statistics, more flexible geospatial outputs, and a range of organisational efficiencies including more efficient linkage of survey and administrative datasets with the Censes.

Summary

A Privacy Impact Assessment, conducted to ensure the protection of privacy and data is an integral part of the process design surrounding the proposal to retain names and addresses from responses to the 2016 Census, has found the retention of names and addresses to be consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

The Privacy Impact Assessment process systematically identifies privacy, confidentiality and security considerations and assesses strategies in place to mitigate or resolve any risks. The Assessment has identified very low risks to privacy, confidentiality and security. The Assessment has concluded that the ABS has implemented robust processes to manage data, protect privacy and guard against misuse of information. These arrangements effectively mitigate the risks, with any residual risks such that the ABS is capable of managing.

Description

As Australia's national statistical agency, the ABS has an enduring commitment to providing trusted statistics and protecting the privacy of individuals and the confidentiality of information supplied by them. These considerations are inherent in the proposal to retain names and addresses from responses to the 2016 Census for statistical and data integration purposes.

The Proposal

Following the completion of Census processing, the ABS will permanently separate names and addresses from other personal and household information on the Census dataset, and store names and addresses separately and securely.

Names will be used to generate anonymised versions of names to use as linkage keys in statistical and research projects that have assessed and approved consistent with *Commonwealth Statistical Data Integration principles, governance and institutional arrangements*. The name and anonymised name files will be stored separately, and will be the responsibility of different teams in the ABS. Neither names nor anonymised names will be part of a Census analytical file.

Addresses and their associated geocodes will be stored separately from the Census dataset, and will be used to support the improvement of geospatial statistics, the ABS Address Register, and other operational efficiencies.

Governance and Management

Retaining names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles. In accordance with its legal obligations, the ABS will ensure that data it receives is kept securely, access is restricted, and that any publication of information does not disclose identifiable information about a person, household or business.

The ABS complies with the mandatory requirements established by the Australian Commonwealth Protective Security Policy Framework, which include implementing governance, physical, and information security measures to protect data held by the ABS. The ABS also takes reasonable steps to comply with the Office of the Australian Information Commissioner Guide to information security and Guide to handling personal information security breaches.

The ABS information technology environment has comprehensive security measures in place, including the most effective Australian Signal Directorate Strategies to Mitigate Targeted Cyber Intrusions and industry best practice. Key measures to safeguard data include high level encryption of data, and an audited linking environment in which staff activity is logged, monitored, and restricted according to role.

The ABS has also been accredited as a safe and effective environment for data integration projects involving Commonwealth data. Consistent with its accreditation status, the ABS has well-established governance infrastructure and procedures to manage the approval, conduct and review of statistical data integration projects undertaken by the ABS.

The ABS will apply internationally recognised best practice separation principles during linkage, analysis and storage of names and addresses to ensure that the files are stored separately, access is granted on an approved need-to-know basis, and that no-one working with the data can view both identifying information (name and address) at the same time as analysis information (such as tenure type or educational attainment).

Risk Identification and Management

The Privacy Impact Assessment identified and categorised a number of potential risks to personal privacy and data security associated with the retention of names and addresses from responses to the 2016 Census. These risks were:

1. Unauthorised access to data stored in the ABS environment by an ABS staff member – Very low risk.
2. Unauthorised external access to data stored in the ABS environment – Very low risk.
3. Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation – Very low risk.
4. Reduction of public trust in the ABS due to privacy concerns – Very low risk.
5. Function creep - unintentional expanded future use of retained name and address information – Very low risk.

The Privacy Impact Assessment process determined that these risks will be effectively mitigated by implementation of the functional separation principle and by existing governance and security arrangements, details of which the ABS has communicated to key stakeholders and the Australian public in the interests of transparency.

Conclusion

In accordance with the above conclusions, the ABS will

7. Retain names and addresses from responses to the 2016.

8. Update the Census Privacy Policy prior to conducting the Census on 6 August 2016 to ensure the Australian public are informed that names and addresses from responses to the 2016 Census will be retained by the ABS for statistical and operational purposes as long as there is a purpose for doing so.

9. Implement business processes which are necessary to manage the separation and retention of names and addresses from responses to the 2016 Census, including separating the internal ownership and responsibility for managing the name file from the area managing the file of anonymised names, and implementing an audit process for Directors responsible for granting access to retained data files.

10. Develop training and support materials for staff accessing name and address data as well as guidelines for ABS Census Interviewers, and publish online responses to frequently asked questions concerning the retention of names and addresses from responses to the 2016 Census to support queries from the public.

11. Conduct an internal audit of the implementation of the above recommendations as part of the internal audit program scheduled for the 2017-2018 financial year.

12. Assign clear responsibility to a Senior Executive Committee for monitoring whether there is an ongoing need for the retention of name and address information.

[redacted]

[redacted]

[redacted]

Item no. 4 – Minutes of the discussion/decision by ELG regarding Item 3.

ELG/2015/26	Database: **ABS Corporate Information** **Executive Leadership Group** **Summary of outcomes - ELG meeting of 8 December 2015** Author Area: **Office of the Statistician**	**8 Dec 2015**

EXECUTIVE LEADERSHIP GROUP - Summary Outcomes

Purpose of Meeting	**EXECUTIVE LEADERSHIP GROUP (ELG)**
Date & Time	**Tuesday 8 December 2015 - 3pm - 4pm**
[redacted]	[redacted]
Chairperson	David Kalisch
[redacted]	[redacted]
[redacted]	

#	Agenda Item
1	**Retention of names and addresses from 2016 Census - Privacy Impact Assessment (PIA) outcomes** [redacted] presented the outcomes of a Privacy Impact Assessment and public consultation process associated with the retention of names and addresses from the Census 2016. Consultation occurred with key stakeholders including Commonwealth and State/Territory Privacy Commissioners (or relevant offices). Three letters were received from the public during the consultation process. The PIA confirmed that retaining names and addresses from Census 2016 is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and complies with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*. ELG agreed that the public good benefits are high while the privacy risks are very low as these risks can be effectively mitigated. ELG agreed to proceed with retention of names and addresses from the 2016 Census. [redacted] ELG asked that the Assistant Minister to the Treasurer be briefed on the decision, provided with the Privacy Impact Assessment and ABS response to the Privacy Impact Assessment, and a copy of the media release that would accompany the public notification of the ABS' decision.

Item no. 5 – ABS internal ‘Privacy Policy’.

Policy and Legislation : Section 04-01

Final
v2014/01
Last Updated:
08 Dec 2015

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	04. Legislation and Legal Issues
Section No. & Title:	01. Privacy Act 1988
Subsection No. & Title:	
Document Version:	2014/01
Status:	*** **Final** ***
Comments:	

Finalised contact details are available for *this section.*

Area Resp. for Updating:	**Office of the Statistician & External Engagement**
General Contact Details	**Head, Audit, Policy and Parliamentary Liaison**
ame:	
hone:	
Specific Contact Details	
ame:	
hone:	
ivision:	
mail:	

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 08/12/2015 02:53 PM
- Body field changed : 6 characters deleted

PRIVACY ACT 1988

Owner: AS OOTSEE
Responsible Director: Audit, Policy and Parliamentary Liaison
Review Date: March 2016

KEY POINTS

1 The *Privacy Act, 1988* (Privacy Act) protects personal information about individuals from mishandling and imposes regulations for collecting, storing, using and disclosing personal information about individuals.

2 Where other legislation (such as the *Census and Statistics Act, 1905* (C&S Act)) imposes stricter requirements (for example, through secrecy provisions), the strictest requirement must be met.

3 Upholding privacy is a core value of the ABS. The ABS adheres strictly to the requirements of the Privacy Act and the C&S Act, both of which underpin our compact with providers. In many cases, the ABS exceeds the requirements of these Acts.

POLICY (INCLUDING DELEGATIONS)

Definitions:

- *May – application of policy is discretional.*
- *Should – application of policy is compulsory unless approved by your AS.*
- *Must – application of policy is compulsory unless approved by Policy Owner.*
-

4 It is ABS policy that all ABS staff must comply with the requirements of the Privacy Act. All Directors should assess their business processes against the requirements of the Privacy Act and mitigate any identified risks.

5 It is ABS policy that name, address and other personal identifiers must be deleted from collected survey and administrative files as soon as practical after processing, unless there is a business need approved by the Statistician via the Program Manager, Governance and Parliamentary Liaison Branch.

6 It is ABS policy that any suspected breaches relating to privacy must be reported to the ABS Privacy Officer as soon as practically possible. The Privacy Officer must investigate the breach and provide recommendations to the Statistician and relevant line management.

7 It is ABS policy that all communication with the federal Privacy Commissioner may only be undertaken by the Statistician; their Executive Assistant; the Deputy Australian Statisticians; the Program Manager, Governance and Parliamentary Liaison Branch; officers of Policy, Legislation and Assurance; or any other officers nominated by the Statistician.

8 It is ABS policy that a privacy impact assessment must be undertaken whenever:

- a survey is undertaken outside of the C&S Act (excluding ABS staff surveys);
- a project, or program, involves high-risk data linkage;
- respondent's personal information will be kept for a prolonged period, or
- if otherwise directed by the Statistician.

It is not necessary to undertake privacy impact assessments for the collection of personal information under the C&S Act.

9 It is ABS policy that personal information about staff must only be collected and used or disclosed to facilitate effective business operations. Personal information collected or stored on ABS managed systems or services must only be available to other staff members with a valid business reason.

10 It is ABS policy that, upon request for access to or correction of personal information from a person under the Privacy Act, all non-statistical data relating to that person must be updated and copies returned to them, if requested. Statistical data is not required to be updated and copies may only be returned in line with the Return of Data to Source policy.

11 It is ABS policy that contractors and subcontractors providing services to

the ABS must be contractually obliged to adhere to the same Privacy Act standards as the ABS, had the ABS been completing the work.

LEGISLATION

What is 'personal information'?

12 Personal information is defined in the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.'

What is 'sensitive information'?

13 The Privacy Act also deals with 'sensitive information' which is a subset of personal information. Sensitive information is defined in the Privacy Act as:

- 'information or an opinion about an individual's:
    - racial or ethnic origin; or
    - political opinions; or
    - membership of a political association; or
    - religious beliefs or affiliations; or
    - philosophical beliefs; or
    - membership of a professional or trade association; or
    - membership of a trade union; or
    - sexual orientation or practices; or
    - criminal record;

  that is also personal information;
- or health information about an individual; or
- genetic information about an individual that is not otherwise
- health information; or
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.'

What are the requirements of the Privacy Act?

14 The Privacy Act provides for principles based protection of individuals' personal information. The Privacy Act includes 13 Australian Privacy Principles (APPs) that apply to the handling of personal information by most Australian, ACT and Norfolk Island public sector agencies, as well as large businesses, all health service providers and some small businesses and non-government organisations. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

15 The APPs are structured to reflect the information lifecycle; from collection, through use, to disclosure, and include the storage and security as well as access to and correction of personal information. The requirements relevant to the ABS for each stage of the personal information lifecycle are:

16 Privacy considerations (APP 1 and 2)

- Manage personal information in an open and transparent way.
- Implement reasonable practices, procedures and systems relating to the functions or activities of the ABS that:
    a) will ensure compliance with the APPs; and
    b) will enable the ABS to deal with inquiries or complaints from individuals about its compliance with the APPs.
- Make a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the ABS available free of charge on the ABS website.
- Except where a legal requirement exists (e.g. compulsory ABS collection) or it is impracticable to do so, give individuals the option of not identifying themselves, or of using a pseudonym, when dealing with the ABS.

17 Collection (APPs 3 and 5)

- Only collect personal information where it is reasonably necessary for, or directly related to, one or more of the functions or activities of the ABS.
- Only collect sensitive information:
    a) where the individual has consented and it is reasonably necessary for, or directly related to, one or more of the functions or activities of the ABS; or
    b) where authorised under law (e.g. C&S Act).
- Only collect personal information by lawful and fair means.
- Only collect personal information about an individual from someone other than the individual if:
    a) the individual consents to the collection; or
    b) it is legal to do so; or
    c) it is unreasonable or impracticable to collect from the individual.
- When collecting personal information about an individual take reasonable steps to notify them about, or otherwise ensure that they are aware of:
    a) the identity and contact details of the ABS;
    b) the fact that the ABS collects or has collected the information and the circumstances relating to that collection:
        i. if collecting from someone other than the individual; or
        ii. the individual may not be aware the ABS has collected the information;
    c) the authority under which the information is being collected (e.g. C&S Act);
    d) the purposes for which the ABS collects the information;
    e) the main consequences (if any) for the individual if all or some of the information is not collected by the ABS;
    f) any third party to which the ABS usually discloses information of the kind collected;
    g) that the ABS APP privacy policy contains information about how the individual may access the personal information about the individual that is held by the ABS and seek the correction of such information;
    h) that the ABS APP privacy policy contains information about how the individual may complain about a breach of the APPs and how the ABS will deal with such a complaint;
    i) whether the ABS is likely to disclose the personal information to overseas recipients; and

j) if the ABS is likely to disclose the personal information to overseas recipients – the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

18 Storage, security, access and correction (APPs 10, 11, 12 and 13)

- Ensure the personal information that the ABS collects is accurate, up to date and complete.
- Ensure the personal information that the ABS uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.
- Protect the personal information held by the ABS from misuse, interference and loss; and from unauthorised access, modification or disclosure.
- Where legal, give individuals access to the personal information that the ABS holds about them on request from the individual.
- Correct personal information held about an individual if either:
  a) the ABS is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
  b) the individual requests that the ABS make a correction to the information.

19 Use and disclosure (APP 6 and 8)

- Only use or disclose personal information about an individual for the particular purpose (the primary purpose) that it was collected.
- Only use or disclose personal information about an individual for another purpose (the secondary purpose) if:
  a) the individual concerned has consented; or
  b) the relevant individual would reasonably expect the ABS to use or disclose the information for the secondary purpose and the secondary purpose is:
     i. directly related to the primary purpose for sensitive information; or
     ii. related to the primary purpose for information other than sensitive information; or
  c) authorised to do so under law (e.g. C&S Act).
- Before disclosing personal information about an individual to an overseas recipient take reasonable steps to ensure that they do not breach the APPs (other than APP1) in relation to the information.

SUPPORTING POLICY INFORMATION (FAQs)

When is information about an individual?

20 The Privacy Act defines an 'individual'. The definition of an individual as 'a natural person' is taken to mean that the Privacy Act, generally, does not protect the personal information of deceased persons. Although the Privacy Act generally only protects the personal information of living persons, C&S Act confidentiality provisions may still apply to personal information about deceased persons.

21 If an individual's identity can be determined from business information (for example, information about sole traders, some partnerships or other businesses), then this information is also personal information and is protected under the Privacy Act. While general information about the business is covered under the C&S Act, it is not covered under the Privacy Act.

What personal information might be collected by business surveys?

22 Examples of personal information that might be collected by a business survey include:

- information about sole traders;
- information about the employees of a business;
- information relating to the clients of a business;
- business names which contain a natural person's name; and
- some business addresses, which are also home addresses.

Additionally, business surveys might collect details for a contact person to follow up with regarding queries.

[redacted]

[redacted]

Does the Privacy Act apply to email addresses?

24 People's email addresses are considered personal information under the Privacy Act when they disclose the person's identity. You should be careful when sending group emails and consider whether you need to use the 'bcc:' field.

How do I make sure that my team's business processes comply with the Privacy Act?

25 To assess your team's business processes against the Privacy Act, Directors should:

- Ensure you are aware of the personal information that your team are responsible for.
- Determine which stages of the privacy cycle your team are responsible for: collection; storage, security, access and correction; use or disclosure; or a combination of these stages.
- Using the Privacy Act requirements outlined in paragraph 15, establish what policies, procedures and training are in place to ensure your team complies with these requirements.
- Assess whether the policies, procedures and training in place, provide adequate protection. If not, identify where there are gaps which could lead to a privacy breach.

- If relevant, develop a plan to address the gaps or ensure that your processes are adapted and adhered to.

What are the consequences if an individual is found to have breached the ABS Privacy Policy?

26 The Statistician will refer the matter to the federal Privacy Commissioner. Pending the outcome of any investigation by the Privacy Commissioner, the matter may also be referred to People Management and Wellbeing for investigation under the Managing Breaches of the Code of Conduct provisions. Possible consequences for the individual and the ABS will range in severity, with civil penalties (including fines and jail time) imposed for serious or repeated privacy breaches.

How do I find the ABS Privacy Officer and what can they help with?

27 The ABS Privacy Officer is located within the Policy, Legislation and Assurance section. To contact the Privacy Officer you can send an email to the Policy & legislation WDB. For urgent queries, you can contact the Director, Policy, Legislation and Assurance.

28 The Privacy Officer can provide assistance to line areas about privacy concerns and answer questions regarding the Privacy Act and its application in the ABS.

What types of personal information does the ABS hold?

29 The ABS deals with personal information about a variety of individuals – providers and respondents (statistical data), staff (employee records), clients and stakeholders (e.g. contact details). The handling of these various types of personal information must be in accordance with the Privacy Act.

How can I notify clients and stakeholders of the fact that the ABS holds their personal information?

30 It is our responsibility to adhere to APPs, which include obligations related to the notification of collection of personal information (APP5), and take reasonable steps to make people aware that the ABS has collected their data, regardless of where the data comes from. The data custodian will often already adhere to the APPs and make people aware that their data is shared with the ABS for statistical and research purposes. If the provision of personal information to the ABS by the data custodian has not been identified, it is the subject matter area's responsibility to consider what reasonable steps (if any) could be taken to make people aware. Reasonable steps will need to take into account whether the personal information is supplied to the ABS on a one off or ongoing basis and could include negotiating with the data custodian to notify people that their personal information is supplied to the ABS.

How can I notify clients and stakeholders of the fact that the ABS holds their personal information?

31 Dealing with clients and stakeholders will often involve handling their personal information, for example, contacting them to respond to a query/request or to consult/engage with them. When inviting client contact, whether through the National Information Referral Service or directly to your area (for example providing contact details on the front page of publications): include a reference to the collection of their personal information and a link to the ABS privacy policy (www.abs.gov.au/privacy). Consider including the ABS privacy policy link and a statement to make new and existing stakeholders aware that your area has collected their personal information when contacting them.

How does the Privacy Act relate to the secrecy provisions in the C&S Act?

32 The C&S Act is much stricter than the Privacy Act in many areas, and the strictest requirement must be always met. For example, the Privacy Act allows for law enforcement bodies to access personal information where it is reasonably necessary for their enforcement related activities, whereas the C&S Act would prevent such access to personal information.

33 As a result of the strict requirements of the C&S Act, the principles relating to the use and disclosure of personal information contained in the Privacy Act have no additional obligations on the information collected under the C&S Act.

Can the C&S Act prevent someone from accessing their personal information?

34 Yes. Information collected under the C&S Act is afforded higher protections than under the Privacy Act. While it is possible for an individual to access their personal information under the C&S Act, the C&S Act only allows for the information collected under it to be returned to the source, that is, the person who provided the information, not the person to whom the information relates. For further information, see the Return of Data to Source policy.

What is a privacy impact assessment and how do I conduct one?

35 A privacy impact assessment looks at a project that (includes the collection, use or disclosure of personal information) from a privacy perspective. The process helps to describe how personal information flows in a project, analyse the possible privacy impacts on an individuals' privacy, and identify options for managing, minimising, or eradicating these impacts.

36 A privacy impact assessment can take many forms. The ABS differentiates between privacy impact assessments that are undertaken in-house for internal consumption (e.g. using a Data Integration Steering Committee template as the tool) and those undertaken externally with findings made available to the public.

37 It is the subject matter area's responsibility to undertake privacy impact assessments. The Office of the Australian Information Commissioner (OAIC) has released a guide which may assist you. The ABS Privacy Officer can also provide assistance to ensure compliance with policy and legislation and must be

consulted regarding the external release of findings from privacy impact assessments.

What is our commitment to the protection of personal information about ABS staff within the organisation?

38 The ABS is committed to only collecting and using or disclosing personal information to facilitate effective business operations, consistent with the requirements of the Privacy Act. If you have any questions or concerns, speak to your Director.

Who has access to my personal information within the ABS?

39 The ABS takes all reasonable and practical steps to ensure the security and privacy of the personal information held. Hard copy records (e.g. personnel files) are stored in a secured environment and access to hard copy and electronic records are limited to authorised staff, and only on 'a need to know' basis. Authorised staff, are staff who have a specific work related requirement and reason to access your personal information (e.g. the Pay and Entitlements, People Management and Wellbeing, and certain IT and Security personnel).

What personal information does the ABS share about me on internal systems?

40 The ABS Corporate Directory contains a basic set of information about staff, necessary to undertake ABS business. This includes their name, email address, phone number, upcoming and current leave, membership of ABS domains, section, location, hours of work, AGS number and position. In addition, the ABS also makes staff photos available through this system on a voluntary basis.

41 The addition of new information to the ABS Corporate Directory would only be implemented following consultation through ABS consultative fora.

42 Where a person holds a position with a decision making delegation or is accountable for large segments of ABS resources, their personal information may be disclosed on the ABS website and on public enquiry. The information disclosed could include a photo of the individual, their name, and a brief resumé. This ensures that individuals with delegations are accountable to the public.

43 In line with public accountability, all staff can also access and view information contained in the many repositories, including:

- Travel Manager,
- certain Workgroup Databases which contain general business emails, and
- certain paper files with records created by individuals.

44 Supervisors, their managers, and areas which provide specific business support are also able to access the following repositories:

- ABS Pay and Leave: this includes name, AGS number, balance by types of leave, years of service, and leave taken.
- Development and Performance Agreements as well as Probationer Reports: this includes name, position, statement of duties and

responsibilities, supervisor's view of performance, and person's view of performance.
- Workplace Collaborative Learning: this includes course attendance and learning needs.
- e-Recruitment: this includes name, resume, statements of claim, assessment by panel, and a record of communication on the selection process. Note that managerial access is limited to the selection panel and staff in National Recruitment.
- Flextime: this includes name, hours work, and leave forms submitted.

Note that access to your personal information for your supervisors and their managers is limited by reporting lines.

What are my manager's confidentiality on obligations for information obtained during discussions with staff?

45 Staff should have a reasonable expectation that sensitive conversations which are held with their manager will not be widely disclosed.

46 Managers have a duty of care to their employees which may necessitate sharing such information with selected areas within the ABS for assistance. As a result, staff should expect that elements of these discussions may need to be shared with the personnel section, their management or other areas as required.

47 Staff must be explicit where they do not want the information to be shared any further.

Will the ABS disclose personal information about staff at the request of law enforcement officers or by court subpoena?

48 The ABS is legally obliged to release non-statistical information when approached by law enforcement, where a warrant has been issued, or to court, where a subpoena has been issued. All such requests to release personal information about staff must be referred to the Director, Policy, Legislation and Assurance.

49 The ABS may release information to law enforcement agencies, without a warrant or subpoena, where the Program Manager, Human Resources Branch or their delegate believes that the release is in the best interest of that staff member.

50 Where an approach is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of an individual, the disclosure may be approved only by the individual; Program Manager, Human Resource Branch; or Director, People Management and Wellbeing.

Can I release the contact details of my work colleagues externally?

51 The work contact details of ABS staff may be released externally when the referral is for work purposes, such as referring people to resolve a query. The personal contact details of staff members (such as home phone number, mobile phone number and address) must never be provided externally, unless approved

by the Program Manager, Human Resource Branch or Director, People Management and Wellbeing.

Who can see my health self-assessment following my successful application for a position in the ABS?

52 The following persons may have access to health self-assessments throughout the recruitment and on-boarding processes:

- National Recruitment Unit staff
- People Management and Wellbeing staff; and
- where appropriate, an independent health assessor engaged by the ABS.

Who can see my police record check application and results?

53 ABS staff in the following sections may have access to police record checks throughout the recruitment and on-boarding processes:

- National Recruitment Unit;
- People Management and Wellbeing; and
- recruitment areas associated with the Census.

Who can see a selection report?

54 A selection report is written by a selection committee and/or scribe. The report is provided to the Delegate who will endorse the final selection decision. The placement panel and Directors involved in the placement process may also have access to selection reports. Applicants may request access to their individual assessment report (if one has been written). In the event of an appeal, a Promotion Appeal Committee, and parties to the appeal may access the full or redacted selection report. In order to undertake administrative actions relating to selections and appeals, the NRU will also have access to the selection report. The SES Liaison Unit has access to selection reports relating to SES recruitment actions.

Who should I contact about access to or correction of personal information?

55 Each Director is responsible for ensuring that any list of contacts that they maintain (e.g. mailing/subscription list, stakeholder engagement details or query/request log) adheres to the APPs.

56 For each of the other types of information listed, you should refer requests to the respective area.

- respondent information - Director, Population Survey Operations;
- client information - Director, Customised and Microdata Delivery;
- staff information - Director, People Management and Wellbeing; Director, Pay and Entitlements; or Director, National Recruitment, depending on the type of staff information needed; and
- other information - Director, Policy, Legislation and Assurance.

How should I respond to an external request for access to or correction of personal information?

57 Respond to requests that relate to non-statistical data by giving access or making a correction within 30 days. Respond to requests for statistical data in line with the Return of Data to Source policy within 30 days and, if refusing to give access or make a correction, respond in writing giving the reason for refusal and the complaint mechanisms available to the person.

When do contractors or subcontractors to the ABS have to comply with the Privacy Act?

58 Always. On occasion, the ABS contracts external service providers to undertake projects that involve being able to see personal information, for example, recruitment processes and HR IT system upgrades. If a contractor or subcontractor has access to personal information then they must comply with the Privacy Act.

How do I correctly use the Sensitive:Personal Email Protective Marker (EPM)?

59 The Dissemination Limiting Marker (DLM) of Sensitive:Personal is used to protect sensitive information only. You should only apply the Sensitive:Personal EPM to emails that contain information classified as sensitive information under the Privacy Act.

REFERENCES AND RELATED INFORMATION

60 *Privacy Act 1988*

61 Australian Privacy Principles – full text

62 Australian Privacy Principle guidelines

63 Privacy Impact Assessment Guide

64 ABS privacy policy

65 Privacy Policy Training Package

For further information, contact:
Head, Audit, Policy and Parliamentary Liaison

Item no. 6 – ABS ‘Security & Confidentiality in Collecting Data Policy’.

Policy and Legislation : Section 10-10

Interim
v2001/04
Last Updated:
03 Sep 2013

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	10. Developing and Conducting Statistical Collections
Section No. & Title:	10. Security & Confidentiality in Collecting Data
Subsection No. & Title:	
Document Version:	2001/04
Status:	*** **Interim** ***
Comments:	

Interim contact details are available for *this section.*

Area Resp. for Updating: **Areas working to Statistician**

General Contact Details **Head, Policy and Legislation**

ame:

hone:

Specific Contact Details

ame:

hone:

ivision:

mail:

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 03/09/2013 11:03 AM

NOTE: THE FOLLOWING POLICY IS CURRENTLY UNDERGOING REVIEW. FOR FURTHER ADVICE ON THE STATUS OF THIS POLICY CONTACT POLICY AND LEGISLATION SECTION.

SECURITY & CONFIDENTIALITY IN COLLECTING DATA

Summary

1 All officers of the ABS are required to uphold the secrecy provisions of the *Census and Statistics Act 1905* and not divulge information obtained under the Act or else face severe penalties. In communicating with respondents to ABS collections it is incumbent on ABS officers to ensure that the methods used provide the security needed to satisfy the secrecy provisions.

ABS Policy

[redacted]

[redacted]

[redacted]

4 It is ABS policy that, using the return to source provisions of section 19 of the Act, for the purpose of data collection and validation, information pertaining to a person (natural or corporate) may be returned by electronic means to the person who supplied it to the ABS only after the identity of that person or another duly authorised person has been verified.

[redacted]

Legislative Requirement

6 The requirement for ABS officers not to divulge to unauthorised persons information collected under the *Census and Statistics Act* is set out in Section 19(1) of the Act as follows:

> "**Secrecy**
>
> **19.** (**1**) A person who is, or has been, the Statistician or an officer shall not, except -
>
> (a) in accordance with a determination; or
>
> (b) for the purposes of this Act;
>
> either directly or indirectly, divulge or communicate any information furnished in pursuance of this Act to any person (other than the person from whom the information was obtained).
>
> (**2**) A person who contravenes subsection (1) or fails to comply with an undertaking of the kind referred to in paragraph 13 (2) (c) given by the person in relation to information disclosed to the person in accordance with a determination is guilty of an indictable offence punishable on conviction by a fine not exceeding $5,000 or imprisonment for a period not exceeding 2 years, or both."

Procedures and Guidelines - Telephones

ABS TELEPHONES A RESPONDENT

Respondent Contacted about an Overdue Return

7 If the respondent agrees to supply the information, details should be taken. If the respondent has doubts about the authenticity of the enquiry, the ABS officer can offer the respondent three methods by which to comply with the requirements:

[redacted]

8 If the respondent engaged in the telephone discussion is unaware of what information had been supplied on the previous return, s/he should not be provided with any details, unless the ABS officer is certain that the information is being supplied only to the "person" (ie natural, or corporate) who provided it.

9 Most ABS collection forms make provision for the business or organisation included in the collection to specify a contact name and telephone number if more information is required or returns need to be queried.

ABS officers should endeavour to speak to the contact officer identified on the form.

10 In some cases the nominated contact officer may not be the person who actually completed the form, and may refer the ABS caller to the person who completed the form. In such cases it is acceptable for the ABS officer to deal with the person(s) to whom they have been referred.

11 In cases where the contact officer/person completing the form is not available, a high degree of discretion is called for in dealing with any other member of the organisation about data contained in the return. ABS officers should seek to contact the owner, the managing director, some other senior manager of the organisation or the accountant. If this person is unable to resolve the problem, s/he should be asked to nominate a responsible person who may be able to help. If there is no suitable person available at the time, arrangements should be made for the ABS officer to call back at a time when a suitable person is available.

12 Even after the bona fides of the person within the respondent organisation have been established, care should be exercised in providing information from a previous return, particularly if it is felt the respondent is simply seeking the information to assist in providing a careless but peremptory estimate.

13 Information supplied by the respondent on a previous return, or amended as a result of subsequent contact between the ABS and the respondent may be provided but, where technically feasible, not data which has been the subject of imputation or which has been amended without input from the respondent.

NOTE: Where editing systems do not provide distinctions between respondent- confirmed edits and office imputations, consideration should be given to incorporating the facility in the next redesign or upgrade of the editing system.

Direct Collection of Data by Telephone

14 The collection of information by telephone is covered by Section 11 (1) of the *Census and Statistics Act* as follows:

> " **Answering of questions**
>
> **11.** (**1**) For the purposes of section 8 or 9, the Statistician or an authorized officer may, either orally or in writing, request a person to answer a question that is necessary to obtain any statistical information in relation to any matter referred to in section 8 or 9."

[redacted]

[redacted]

[redacted]

[redacted]

18 If a respondent shows hesitation about the provision of information for any collection by telephone arising from uncertainty or concern about the bona fides of the ABS caller, or for any other reason, explicit or otherwise, then procedures similar to those presented in para 7 above should be followed.

19 If the respondent is unaware of what information had been supplied on the previous return, the same policy applies as when telephoning for an outstanding return (see para 8 above).

Querying returns

20 Query action is usually initiated in respect of information on a current return, but could necessitate reference to the previous return(s) for comparison of previous period(s) with current period information. In all such cases ABS officers must speak to one of the actual persons outlined in para 11 above. If none of those people are available, the query should be conducted by mail, addressed to a specific person or position.

RESPONDENT TELEPHONES THE ABS

21 A call may originate from the respondent, employee, accountant, owner etc. On no account is information on a return to be disclosed over the telephone until the bona fides of the caller have been established. This can be achieved by the ABS officer requesting the caller to quote the SRN or IRID printed on the form.

22 If the bona fides of the caller cannot be established at this point, the respondent should be called back on the number quoted on the latest return and the inquirer should be advised of ABS policy in this regard (see para 2 above) and asked to submit the request in writing and preferably signed by the person who submitted the return.

23 If there has been a change of ownership in the organisation and a request is made for data supplied on a return provided under the previous ownership, it is acceptable to comply with the request provided it is made by the same person who supplied the original data and that person's identity has been established.

24 In all other cases where a change of ownership is known to have taken place information should not be provided.

NOTE: a There have been occasions when new owners have attempted to obtain historical data for use in court cases against the previous owners. For this reason, extreme care is called for in the handling of requests when it is known that there has been, or may have been, an ownership change.

b ABS records may indicate a change of ownership, artificially resulting from changes to SRNs following the creation of Management Units on IRIS. In these cases, ABS officers should be sensitive about the public relations consequences if data is withheld without justification.

ONE OFFICE OF THE ABS TELEPHONES ANOTHER

25 Details of a confidential nature should not be discussed by telephone unless the ABS officer making the call is known to be an ABS officer by the officer receiving the enquiry, and the reasons for the request are justified.

26 In dealing with statistical returns, the quoting of SRNs and IRIDs or some other unique identification number is sufficient to establish the officers' bona fides.

27 When in doubt the officer receiving the call should arrange to return the call, verifying the telephone number against the internal telephone directory or switchboard of the relevant office before calling back.

Procedures and Guidelines - Telex and Facsimile

Background

28 Unlike telephones, errors made in the keying of the Telex or Facsimile number can remain unknown to the sender until after the information has been transmitted. Telephone calls, once answered, enable verification of the called number before any further information is communicated and therefore pose little risk of a breach of confidentiality once the bona fides of the person handling the call have been confirmed.

29 With Telex and Facsimile facilities, information is frequently transmitted to unattended receiving stations sited in locations without restricted access. Errors made in the keying of Telex and Facsimile numbers and which remain undetected until after the transmission of the message can not only result in the transmission of information to the wrong organisation, but also result in access to the printed transmission by individuals who have uncontrolled access to the unattended facsimile or Telex machine.

ABS Transmissions to Respondents

30 There is no restriction to the sending of blank forms to respondents by facsimile.

31 Because of the risk of an error in the keying of a facsimile number, and the risk of uncontrolled access to confidential information transmitted to a correct addressee arising from unattended facsimile machines, a completed return should not be transmitted to a respondent except where there has been agreement by the ABS and an appropriate representative of the respondent organisation (see para 8 above) and procedures are in place to minimise the possibility of the information being transmitted to the wrong organisation.

32 Methods available to minimise errors in transmission include verification of the respondent's facsimile (telex) number through the Telecom National Business Directory and the requirement that two ABS officers be in attendance when sending a facsimile (or telex), one to dial the other to verify.

33 All facsimile and telex messages to and from respondents should be marked "STATISTICS-IN-CONFIDENCE".

Respondent Transmissions to ABS

[redacted]

35 Respondents should be advised, when sending information via facsimile or telex, to verify the ABS number(s) and, if possible, notify the ABS contact officer for the collection of the transmission date and time.

36 As an additional protection and to provide further reassurance to respondents, facsimile facilities used by an ABS subject matter area for the transmission or receipt of confidential information should be under the direct control or supervision of that subject matter area.

A general ABS facsimile number should not be used for the transmission of data to the ABS.

37 To assist in this process ABS forms and reminder letters/cards should not include ABS general facsimile numbers.

Transmissions Between ABS Offices

38 To minimise the risk of incorrect transmissions confidential information between ABS offices should, where practicable, be transferred using the ABS mainframe or via electronic mail on the LAN.

FREQUENTLY ASKED QUESTIONS

Why do we offer the electronic collection of data to respondents?
notes:///CA255E8A0003F1E8/D0FCD1F53943D2BECA2570650016FE52/AC7CB1E0627E59D2CA2567450009EECA

39 The ABS has developed its current collection techniques as technology, community preferences and requirements have progressed. Our methods have evolved over many years to include telephone, mail, fax, CD-Rom, and email into the Secure Deposit Box. In turn, our business practices have become more efficient by using these technologies. More recently, the ABS introduced eCensus on the internet for the 2006 Census as an on-line alternative to paper-based forms.

How does this policy relate to the Electronic Transactions Act?
notes:///CA255E8A0003F1E8/D0FCD1F53943D2BECA2570650016FE52/AC7CB1E0627E59D2CA2567450009EECA

40 *The Electronic Transactions Act* facilitates the use of electronic communication when supplying information to the Commonwealth. It requires the Commonwealth to accept electronic communications to satisfy any legal obligations imposed under Commonwealth laws. Therefore, electronic documentation and signature is a legal document and holds the same legal position as a written document and signature. The ABS works in accordance with the Electronic Transactions Act by accepting electronic documentation, while maintaining the security of all information provided to the ABS.

References and Related Information

41 If you are having any technical difficulties accessing this document eg. broken links, please contact the Audit, Policy and Parliamentary Liaison Section.

Back to top

For further information, contact:
Head, Policy and Legislation

Item no. 7 – ABS ‘Information Security Policy’.

Policy and Legislation : Section 16-03

Final
v2013/01
Last Updated:
09 Dec 2014

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	16. Security
Section No. & Title:	03. Information Security Policy
Subsection No. & Title:	
Document Version:	2013/01
Status:	*** **Final** ***
Comments:	

Finalised contact details are available for *this section.*

Area Resp. for Updating:
General Contact Details **Director IT Security**

ame:

hone:
Specific Contact Details

ame:

hone:

ivision:

mail:

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 09/12/2014 04:05 PM

Introduction

1. Information Security encompasses those measures by which ABS sensitive/classified information stored on any media, is identified and appropriately protected having regard to its level of sensitivity or classification.

2. ABS sensitive/classified information falls within four broad groupings:

- Information provided by respondents in compliance with the *Census and Statistics Act 1905* and iterations of that information;
- Working papers and drafts containing sensitive/classified information and embargoed statistical information;
- Certain Corporate Information such as:
    a. personal information in respect of ABS employees, contractors and applicants for employment
    b. information relating to the operations/administration of the ABS such as tender/submissions, responses and evaluations, sensitive industrial relations matters, some matters relating to leasing of premises, and procedural documentation
    c. certain technical documents relating to IT systems, software, procedures and practices
- Information received from other Government Agencies e.g. Cabinet documents.

3. The Protective Security Policy Framework (PSPF) sets out standard Government practices applied to the protection of sensitive/classified information, and is supported by the legislative provisions of the Crimes Act which include penalties for unauthorised disclosure of information.

4. The *Census and Statistics Act 1905* contains the legislative provisions for the protection of information furnished under that Act and the penalties for its unauthorised disclosure.

5. Where possible and appropriate the practices set out in the PSPF will be applied to the protection of ABS sensitive information.

6. Security of ABS Publications is governed by standard ABS practices for the protection of information contained within publication working papers, draft and embargo copies. These practices should be consistent with the requirements of the PSPF but must take into account the unique requirements of the ABS publication life cycle.

Information Security

7 Access to any sensitive/classified information in the possession of the ABS is only authorised if the intended access is permitted by legislation and:

I. there is no conflict of interest;

II. there is a valid 'Need to Know'; and

III. an appropriate ABS Security Clearance is held where the information has a national security classification.

8 A person has a genuine 'Need to Know' if, without access, they would be hindered in the performance of their duties or the provision of services to the ABS. This 'Need to Know' principle is to be applied prior to access to any sensitive information in the possession of the Australian Statistician.

9 Except where ABS security policy states to the contrary, the information classifications categories and definitions, and information handling, storage, movement and destruction procedures set out in the Protective Security Policy Framework & Information Security Manual will be used as the basis for the protection of all:

I. ABS Corporate information; and

II. Information received from other Commonwealth Agencies.

10 The "Guidelines for Processing and Release of MEI's" are to be used as the basis for the protection of all information contained within working papers for, and draft and embargo copies of, all ABS publications. (Notes Link) (Subject: Guidelines on Processing and Release of MEIs; Database: ABS Corporate Manuals; Author: Bryan Hogan; Created: 20/11/2001)

11 The guidelines contained in "Security & Confidentiality in Collecting Data" are to be used as the basis for the protection of all information provided under the *Census and Statistics Act 1905*, and iterations of that information. Notes Link (Subject: Security & Confidentiality in Collecting Data; Database: ABS Corporate Manuals; Author: Paul Fairhall; Created: 31/03/1999)

12—— The 'clear desk, clear screen policy' Notes Link requires that at no time, including short absences, is sensitive information to be left unattended where it may be accessed by others who are not authorised.

13 Team or Sections handling any of the four categories of ABS sensitive information provided above, must develop a Team or Section Security Plan detailing the appropriate management and security of such information in line with 'need-to-know' principles. The Plan must ensure ABS employees are aware that, prior to leaving their area/workstation, the information is appropriately secured and detail how this can be implemented, including definitions of what constitutes short and long absences.

14 During longer absences and close of business sensitive/classified data must be appropriately secured in line with the agreed team/section security plan.

15 All employees must ensure that their network access is protected by activation of a screen saver on the PC/notebook with password for absences during the work day or by logging off at close of business.

16 Persons providing goods or services under a contract with the ABS must comply with the 'clear desk,clear screen policy' in respect of any ABS sensitive/classified information they are authorised to access.

17 Where an employee, or persons providing goods or services under a contract with the ABS, becomes aware of any loss, unauthorised access, or disclosure of, ABS sensitive/classified information they are to complete an security incident report immediately using the following link Notes Link to the Security Incident Reporting System DB, and selecting 'Create', then 'Incident Report'.

18 If the incident is serious, cannot be contained, or an incident report cannot be completed immediately, they are to advise Central Office or Regional Office security personnel as soon as possible. Contact details are available via the Security Assistant Notes Link.

Sanctions for not complying with ABS Security Policies

19. All ABS staff must read and comply with this policy and supervisors must draw it to the attention of staff under their supervision. Any failure to comply with this policy may result in disciplinary action being taken under the *Public Service Act 1999*, which provides for penalties up to dismissal where misconduct is proven, and/or in the case of possible illegal conduct, referral of the matter to the police.

For further information, contact:
Director IT Security

Item no. 8 – ABS ‘Clear Desk, Clear Screen Policy’.

Policy and Legislation : Section 16-10

Final
v 2013/01
Last Updated:
30 Mar 2016

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	16. Security
Section No. & Title:	10. Clear Desk, Clear Screen Policy
Subsection No. & Title:	
Document Version:	2013/01
Status:	*** **Final** ***
Comments:	

Finalised contact details are available for *Chapter 16 'Security'*

Area Resp. for Updating: **Technology Services Division**

General Contact Details **Director, Security**

ame:

hone:

Specific Contact Details

ame:

hone:

ivision:

mail:

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 30/03/2016 04:42 PM
- Body field changed : 242 characters deleted

Clear Desk, Clear Screen Policy

Principles

1. Protective Security Policy Framework: Physec 6 directs Agencies are to implement general control policies including a Clear Desk and Clear Screen Policy.

2. Clear Desk Policy is defined as "A policy requiring a person to ensure that security classified information and other valuable resources are secured appropriately when the person is absent from the workplace
3. Clear Screen Policy is defined as "A supplementary policy to the clear desk policy that requires a person to ensure that information on ICT equipment is secured appropriately when the person is away from the workstation, e.g. by locking the ICT equipment.

3. The purpose behind implementing a Clear Desk and Clear Screen policy is to both meet the requirements set out in the PSPF and protect the ABS reputation,

staff, assets, both corporate and personal, and information from compromise and/or theft.

Responsibilities

4. All ABS employees are responsible for the security of sensitive/classified information and/or assets under their control.

5. Managers carry the responsibility for determining which of their staff have a need-to-know and require access to sensitive/classified information and for ensuring the work area has a security plan.

Requirements

6. During absences from the workplace, employees must ensure that sensitive/classified information is secured appropriately and there are no “attractive assets” visible.

7. To assist staff in meeting the clear desk policy, sensitive information must be stored in an appropriate manner, whether for a short, medium or long term absence. As the sensitivity of information varies, work areas are in the best position to determine what is a short or long term absence and the appropriate means of securing in these instances. Work areas should also ensure there is an appropriate system in place for checking the workplace at close of business to ensure information/assets are secured.

8. As stated in of the Information Security Policy Notes Link, staff must ensure protection from unauthorised access to any electronic system or network to which they have been connected or are responsible for by either locking the computer through activating the screen saver or logging off.

9. During short absences, employees could turn over or cover classified information, or inform another employee that they are leaving and lock their computer access. The practice undertaken will depend on the sensitivity of the information and the directions of the Director of the area.

10. For long absences, it would mean locking the computer, securing assets and sensitive/classified information by locking away in a in a locked cabinet/container/room.

11. At the close of business each day, staff should take precautions to ensure that all official information, especially classified/sensitive information, is protected from unauthorised access.

12. The following should be observed by all staff as part of an effective close of business procedure:

- logging off all computer systems
- ensuring there is no sensitive/classified information left out in the workplace (paying special attention to shared network printers)

- Personal Electronic Devices (this excludes notebooks) and Portable Storage Devices, are secured appropriately (for example: in a locked cabinet/container/room) to mitigate potential loss and/or unauthorised data access
- ensuring there is no sensitive /classified information in waste-paper bins
- ensuring that whiteboards and other displays do not show any classified/sensitive information (special care needs be taken with electronic whiteboards i.e.: storage or disposal of printout, and erase or cover board when not in use)
- ensuring security containers are locked
- ensuring that keys to containers and segregated areas are secure
- if required, ensuring windows and doors are locked.

13. The Protective Security Section are able to provide advice on options for securing sensitive/classified and/or assets.

For further information, contact:
Director, Security

Item no. 9 – ABS ‘Return to Source Policy’ (expired May 2016)

Policy and Legislation : Section 12-03

Final
v2010/01
Last Updated:
21 Aug 2013

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	12. Confidentiality and Disclosure
Section No. & Title:	03. Return of Data to Source
Subsection No. & Title:	
Document Version:	2010/01
Status:	*** **Final** ***
Comments:	

Finalised contact details are available for *this section.*

Area Resp. for Updating:	**Office of the Statistician & External Engagement**
General Contact Details	**Head, Audit, Policy and Parlimentary Liaison**
ame:	
hone:	
Specific Contact Details	
ame:	
hone:	
ivision:	
mail:	

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 21/08/2013 09:55 AM

RETURN OF DATA TO SOURCE

KEY POINTS

1 The secrecy provision, Section 19 of the *Census and Statistics Act 1905* (C&S Act), generally prohibits the disclosure of information furnished in pursuance of the Act except as permitted by the Act. However the return of information to the person from whom it was obtained is specifically excluded from this secrecy requirement. This is referred to as 'return to source' and it is this provision which enables the ABS to query data provided by respondents directly with the respondents involved. The return to source provision also enables the ABS to prepare 'customised reports' (i.e. reports that compare a respondent's results with aggregate statistics for a group of respondents), and to give respondents access to their own data if they request it.

2 The return to source provision does not provide any limitations on the type of information that can be returned, provided the information was obtained from the respondent and as long as the information is returned to the person who originally supplied it. However, the ABS can return information that has been coded or edited for internal consistency using information already supplied by the same person; e.g. coding an address to statistical local area, or cause of death coding.

3 Where two data sources are combined, or data are supplied by one source and amended using information from another source, the resultant data cannot be returned under the return of data to source provision.

POLICY (INCLUDING DELEGATIONS)

4 Consistent with our legislation, it is ABS policy that ABS staff must ensure that the information is returned to an appropriate person. In all cases, the bona fides of the person to whom information is being returned, must be established before any information is provided. Judicious questioning should be used to establish this.

5 It is ABS policy that information supplied:

I. by sole proprietors, can only be returned to the proprietor who initially provided the information. Information cannot be provided to a subsequent owner of the business or an employee or agent of the business, such as an accountant.

II. by an individual who has provided information about themselves, can only be returned to that person.

III. by an individual who has provided information about another person (e.g any responsible adult (ARA) methodology), the information can only be returned to the person who supplied the information, not the person to whom the information is about. (See the Frequently Asked Questions below for how this relates to the Privacy Act.)

IV. by an individual who acts as an agent for another person (e.g. an interpreter or a doctor), can only be provided to the person about whom the information is provided, and not their agent. (See Frequently Asked questions below for more information).

V. by a partnership, can only be returned to the person who provided the information, and not to any other partners.

VI. by companies or other bodies corporate, can be returned to such a corporate entity while it continues in existence. Information can be returned to the person who provided the information or, if discretion is exercised, to the contact officer named on the ABS questionnaire (such as a chief financial officer or payroll manager), or to a responsible person (such as the managing director, or the chief accountant), within the company. If a takeover has occurred, and the original corporate entity ceases to exist, information previously reported should not be returned to the entity which has acquired the original business.

VII. as administrative records or register-based datasets, can only be returned to the business or organisation (often a government agency) that provided the information to the ABS.

Requests for ABS survey information to be returned to source

6 In the case of requests from persons or businesses for data to be returned, it is ABS policy that written confirmation should be sought from that person or business. This written confirmation can be in any form. In straight-forward cases, an email request is sufficient, but in more complex cases a Statutory Declaration may be required.

7 It is ABS policy that the only information that may be returned to source is the information which was originally provided to the ABS. That is, the return to source provision is limited to the information that was obtained from the respondent. However, the ABS can return information that

has been coded or edited for internal consistency using information already supplied by the same person; e.g. coding an address to statistical local area, or cause of death coding.

8 Care must be taken returning data held in electronic format to ensure that only the original file received from the respondent is returned. If the original file is unavailable, contact the Audit, Policy and Parliamentary Liaison Section for advice.

Requests for administrative datasets to be returned to source

9 It is ABS policy that in the case of administrative datasets or register-based information, the 'source' is regarded as the organisation (often a government agency) that provided the information to the ABS. The person or business who provided the information to the government agency is not the source. (See paragraph 26 in the Frequently Asked Questions section below for more information on querying data with the person or business who provided the information to the organisation/government agency in the first instance.)

10 The only information that can be returned to the source is the information which they originally provided to the ABS. However, the ABS can return to an agency information that has been coded or edited for internal consistency using information already supplied by the same agency; e.g. coding an address to statistical local area, or cause of death coding. Information not resulting from the original dataset cannot be returned to the source (e.g. if that dataset has been linked with another dataset).

11 The entity about whom information relates, that is, the business, organisation or agency which supplied it to the ABS source in the first instance, can be queried under Section 19(1) of the C&S Act. However, it is ABS policy that such querying is limited to information of a non-personal or domestic nature, and where at least one of the following applies:

I. the original supplier of the information is made aware on the collection instrument that the data was likely to be provided to the ABS; and/or

II. the passing on of information to the ABS is written into the collecting agency's legislation.

12 It is ABS policy that any new proposals to return partial or entire administrative datasets to their source must be approved by the Statistician, through the Audit, Policy and Parliamentary Liaison Section. Once approved, and if ongoing, these should be reviewed every three years and approved by the relevant First Assistant Statistician.

13 For the purposes of return of data to source, each department, agency, and government business undertaking must be treated as a separate entity (i.e. data supplied by one department or agency can be returned, under the return of data to source provisions, only to that department or agency).

Delegations

14 There is no formal delegation specified in the legislation for return of data to source. It is ABS policy that, other than the approval level specified in paragraph 12, the level of approval required for any request for information to be returned to source depends on the circumstances of each case, and is determined locally by collection areas.

15 It is ABS policy that supervisors and team leaders should ensure that the legislative obligations and local delegations regarding the return of data to source provision are understood by all survey collection and processing staff.

ABS edit queries

16 It is ABS policy that the ABS should aim to use the contact person listed on the ABS survey form to resolve any editing queries. Where the contact person is not available, the ABS should only contact the alternatives defined in paragraph 5.

LEGISLATION

17 19 (1) A person commits an offence if:

(a) the person is, or has been, the Statistician or an officer; and

(b) the person, either directly or indirectly, divulges or communicates to another person (other than the person from whom the information was obtained) any information given under this Act.

18 19 (2) Subsection (1) does not apply if the person divulges or communicates the information:

(a) in accordance with a determination under section 13; or

(b) for the purposes of this Act.

FREQUENTLY ASKED QUESTIONS

Can information be returned to a child whose parent has answered survey questions on their behalf?

19 When a parent responds on behalf of a child (i.e. proxy responses), the parent is considered to be the source of that information. Therefore, the information can only be returned to the parent, not the child.

In the C&S Act, why are only 'persons' mentioned in the return of data to source provision?

20 According to the *Acts Interpretation Act 1901* the term person "includes a body corporate, office, commission, authority, committee, tribunal, board, institute, organization or other body however described."

How does the return to source provision interact with the Privacy Act and ARA methodology?

21 While the Privacy Act states that individuals should have access to personal information about themselves, it doesn't allow for disclosure of information if it is restricted by other commonwealth legislation. In terms of the ARA methodology used by the ABS, the C&S Act only allows information to be returned to the source. That is the person who gave the information, not the person to whom the information relates. As the C&S Act is commonwealth legislation, these provisions override the Privacy Act.

Why are agents treated differently to ARA methodology?

22 Agents (such as interpreters) provide information to the ABS on behalf of a person selected in the survey. Therefore the person selected has authorised the information given to the ABS. However, the information given by an ARA has not been authorised by the other party.

What sort of information is covered by return of data to source (e.g. can a spreadsheet or the name of a contact be returned)?

23 The return of data to source provision does not provide any limitations on the type of information that can be returned, provided the information was obtained from the respondent, and as long as the information is returned to the person who originally supplied it. See the policy section above to determine the source of the data.

What happens if a department changes name or responsibilities?

24 There may be instances where a government agency undergoes a change in name, a change in responsibilities, or a movement in work between agencies. In the case of an agency undergoing a name change only, then data can continue to be returned to this agency. In all other cases, the Audit, Policy and Parliamentary Liaison Section will determine whether data can be returned to source.

Can several administrative datasets from the same organisation be integrated and then returned to source?

25 Generally, no. Arrangements for return to source of integrated datasets should be viewed cautiously, especially as the merged datasets may have been obtained under different legislative arrangements. In addition, identifying duplicate records on administrative datasets could assist with compliance sanctions for an individual (e.g. someone appearing on two different payments streams). Therefore any proposals to enter into any such arrangement should be approved by the Statistician, through the Audit, Policy and Parliamentary Liaison Section.

In cases where a government department/entity passes on information to the ABS that was provided to it by a respondent, can the ABS also query the original provider?

26 Section 19(1) of the C&S Act does not prevent the ABS from querying the original supplier of data (e.g. the importer/exporters in the case of Customs data). It is ABS policy that where the original provider of the data is made aware that the data is being passed onto the ABS on the collection instrument, or the provision of data to the ABS is written into the collecting agency's legislation, querying data is considered conducive to the collection of accurate statistical information. It is therefore covered under the s 19(2)(b), which provides that s 19(1) does not apply if the information is divulged or communicated 'for the purposes of the [C&S] Act. However, under ABS policy, this does not apply to information of a personal or domestic nature, as this data is considered too sensitive and disclosure may lead to privacy concerns.

27 *Census and Statistics Act 1905*

28 Pro forma letter checking for changes in ownership

29 Statutory Declaration

30 In the first instance, any queries relating to the application of this policy should be discussed with your own line management. Any further queries should then be directed to Audit, Policy and Parliamentary Liaison Section.

31 If you are having any technical difficulties accessing this document e.g. broken links, please contact the Audit, Policy and Parliamentary Liaison Section.

Item no. 10 – ABS ‘Return to Source Policy’ (from May 2016)

Policy and Legislation : Section 12-03

Final
v 2016/01
Last Updated:
24 May 2016

Manual Category	**B. Policy and Legislation**
Manual ID - No & Title:	**Policy - Policy and Legislation**
Chapter No. & Title:	12. Confidentiality and Disclosure
Section No. & Title:	03. Return of Data to Source
Subsection No. & Title:	
Document Version:	2016/01
Status:	*** **Final** ***
Comments:	

Finalised contact details are available for *Chapter 12 'Confidentiality and Disclosure'*

Area Resp. for Updating:	**Office of the Statistician & External Engagement**
General Contact Details	**Head, Audit, Policy and Parliamentary Liaison**
ame:	
hone:	
Specific Contact Details	
ame:	
hone:	
ivision:	
mail:	

To be notified when a change to this document is published,
register yourself, your workgroup or your workgroup database email address in the table below.

- Click in the left hand margin to select an existing entry
- Press F9 if your registration doesn't appear automatically

The documents linked here:

- offer guidance on related matters
- when changed will demand a review and possible updating of this document and/or
- will need to be reviewed and perhaps updated as a consequence of changes to these documents.

Policy

Standards

Definitions

Procedures

Other links

Last modified by [redacted] on 24/05/2016 10:38 AM

Return to source policy

Policy Name: Return to source

Level 1 policy owner: Australian Statistician

Level 1 approved: 20 May 2016

Purpose

Information collected by the ABS for statistical and/or research purposes is subject to stringent confidentiality to maintain privacy, community trust and integrity. Return of collected information to its source is required in some instances to enable validation and to reduce respondent burden, for example through the pre-population of collection forms.

Scope

This policy applies to all information collected by the Australian Bureau of Statistics for statistical or research purposes protected by the secrecy provisions of the *Census and Statistics Act 1905*.

Principles

The principles that underpin this policy are:

1. Information collected under the authority of the *Census and Statistics Act 1905* may be returned to its source consistent with, and for the purposes of, the Act to:

    a. validate and/or enhance the quality of information received;

    b. pre-populate collection forms to reduce respondent burden;

    c. provide respondents with access to the information they have provided; and/or

    d. prepare customised reports.

2. In certain circumstances the ABS can return information to another person. These are where:

    a. that person is an employee of the entity that supplied the information; or

    b. the relevant Deputy Australian Statistician has approved the provision of information to that person where it is consistent with, and necessary, to support the functions of, the *Census and Statistics Act 1905*.

    Further details of these circumstances are outlined in Level 2 of this policy.

3. Reasonable steps are taken to protect the confidentiality and privacy of information returned, in accordance with the *Census and Statistics Act 1905* and the *Privacy Act 1988*.

4. Information returned to source in accordance with this policy is considered exempt from embargo.

5. The relevant General Manager may approve the return of partial or entire unit record or aggregate administrative, transactional and other datasets to their source.

6. Where administrative data has been collected from an original provider by a third party entity and then provided to the ABS, the relevant General Manager may approve the querying of data with the original provider.

7. The relevant General Manager may approve the pre-population of forms as outlined in this policy.

Definitions

1. A **person** can be an individual, body corporate (company, corporation) or body politic (local council, state, territory or Commonwealth department or agency), or unincorporated business.

2. **'Reasonable'** is based on ordinary meaning, being based upon or according to reason and capable of sound explanation. It is an objective test and a question of fact in each individual case that has regard to how a reasonable person, who is properly informed,

would be expected to act in the circumstances.

3. **'Reasonable steps'** is an objective test, and is to be applied in the same manner as 'reasonable'.

4. An **original provider** is the original source of the information in relation to administrative and transactional data, e.g. a customs agent provides information to Customs which then provides an administrative dataset to the ABS.

5. An **entity** is a public or private sector organisation located within Australia or internationally.

6. An **alternate officer/contact** in a body corporate or body politic could be a different officer of the same function, or an officer of senior position with a portfolio related to the information returned.

7. **Pre-population of a survey form** is the inclusion of information, obtained from a previous iteration of the same survey or information obtained from another survey or organisation, in a form to be provided to a respondent. A form may also be pre-populated with information obtained from the ABS survey frame source, for example the ABS Business Register.

8. **Personal information,** as defined in the *Privacy Act 1988*, means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    a. whether the information or opinion is true or not; and

    b. whether the information or opinion is recorded in a material form or not.

    For the purposes of the *Census and Statistics Act 1905*, personal information also includes information of a domestic nature.

Level 2 policy owner: General Manager, Industry Statistics Division

Level 2 approved:20 May 2016

Level 2 Delegations

1. The General Manager, Industry Statistics, is accountable for the currency of Level 2 return to source arrangements and delegations and may amend them at any time provided they remain consistent with Level 1 return to source principles and arrangements approved by the Australian Statistician.

2. *Information collected under the authority of the Census and Statistics Act 1905 may be returned to its source consistent with, and for the purposes of, the Act.* The information returned may not be edited or modified using information acquired under the *Census and Statistics Act 1905* from another person or entity.

3. *The ABS can return information to another person or entity. This can occur where:*

    a. *that person is an employee of the entity that supplied the information; or*

    b. *the relevant Deputy Australian Statistician has approved the provision of information to that person where it is consistent with, and necessary, to support the functions of, the Census and Statistics Act 1905.*

<u>Administrative and transactional data</u>

4. The source of an administrative or transactional dataset is defined as the entity that provided it. Information may be returned to an alternate officer/contact within the entity that provided it if the person performs the same function as the person that provided the information, or is a more senior person in the same hierarchy.

5. *The relevant General Manager may approve the return of partial or entire unit record or aggregate administrative, transactional and other datasets to their source* provided that:

    a. if datasets have been aggregated, they do not contain:

        i. information acquired under the *Census and Statistics Act 1905* from another person or entity

        ii. additional information from another person or entity

    b. methods applied to the data are available publicly.

6. Ongoing requests, once initially approved by the relevant General Manager, are to be reviewed and approved by the relevant Program Manager every three years.

7. *Where administrative data has been collected from an original provider by a third party entity and then provided to the ABS, the relevant General Manager may approve the querying of data with the original provider* provided:

a. the entity which provided the administrative data has advised the original provider that their data will be passed on to the ABS for statistical purposes and the ABS may query them directly; and

b. the entity which provided the administrative data consents in writing that the ABS may query the original provider; and

c. arrangements are in line with other existing arrangements/agreements between the ABS and the entity which provided the administrative data.

Survey and other directly collected data

8. *The relevant General Manager may approve the pre-population of forms as outlined in this policy.*

9. Approval for all other return to source requests may be determined by survey collection areas and/or Data Acquisition and Provider Management Branch in accordance with the guidelines below.

Returning information to an appropriate individual

10. Information from a *household* or an *individual* may only be returned to the individual who provided the information unless otherwise enabled under paragraph 3 above.

11. Information from an *individual who acts as an agent* for another individual (e.g. an interpreter or doctor) may only be returned to the individual about whom the information is provided, and not their agent unless otherwise enabled under paragraph 3 above.

12. Information from an *unincorporated business* may be returned to the individual who provided the information. Partnerships and sole traders should be treated as individuals (paragraph 10).

13. Information from a *body corporate or body politic* may be returned to the officer who provided the information, or to an alternate officer/contact.

14. If a takeover has occurred, and the original entity ceases to exist, information previously reported should not be returned to the new owner.

Pre-population of survey forms

15. Information collected as part of an ABS survey may be returned to the individual who supplied it through a pre-populated form for the same survey.

16. Pre-population of forms using the data obtained from another survey or organisation are permitted in certain circumstances including where:
    a. it is necessary to use that data to inform the activity to be surveyed; and
    b. information in the pre-populated form is:
        i. personal information relating to the person who supplied the information;

        ii. disclosed in a manner not likely to enable the identification of the person who provided the information; or

iii. information obtained from the ABS Business Register (the survey frame).

Actions not permissible under this policy

17. This policy does not permit the return of information:

- that has been edited using other information collected under the *Census and Statistics Act 1905*;
- collected from a partnership to a partner, other than the individual who provided it;
- collected from an individual which pertains to a second individual, to that second individual (e.g. advising a person that they have been identified as a smoker by another person responding to an ABS survey is not permitted); or
- collected outside the *Census and Statistics Act 1905* for any purpose, including for the purpose of supporting data integration activities and/or the provision of services. The return of this information is subject to the requirements of the *Privacy Act 1988*.

Additional materials

Privacy policy Notes Link
Embargo policy Notes Link

Frequently Asked Questions

For further information, contact:
Head, Audit, Policy and Parliamentary Liaison