2016 Census Review
Senate Standing Committees on Economics
GPO Box 6100
Canberra ACT 2600

20 September, 2016

RE: 2016 Census Review

My name is Dr. Cassandra Cross and I am currently a Senior Lecturer with the School of Justice, Queensland University of Technology. I teach undergraduate subjects related to policing, crime prevention and cybercrime, with my own research specialisation in the area of cybercrime, specifically online fraud victimisation and identity theft. I have been researching in these fields since 2008, and my work has led to the receipt of a Churchill Fellowship in 2011, where I travelled to the United Kingdom, United States of America and Canada to explore how these three jurisdictions are responding to the problems and challenges posed by online fraud. I have also been awarded two federal government Criminology Research Grants. The first was in 2013, to complete a project entitled *Improving the responses to online fraud: An examination of reporting and support*. This was the first Australian study to specifically examine the reporting experiences and support needs of online fraud victims. This project is complete with findings publicly available. The second was in 2015, and was entitled *Addressing the needs of identity theft victims: A multidimensional view*. This project is currently in progress and will track 200 identity theft victims across a 12 month period to analyse their journeys in seeking to restore a compromised identity. As part of this study, my colleague and I have undertaken an analysis of 1499 cases of identity theft across a number of variables to determine if how an identity is compromised has an impact on the subsequent harm experienced by individual identity theft victims. I will refer to these results in the body of this submission. Within my work, I also speak at many community events on the broader topic of cyber, particularly targeted at seniors. As part of this, I am the author of a training package entitled *Seniors Online Security*, which seeks to improve the knowledge and awareness of seniors to internet safety across five topics: computer security, identity theft, social networking, fraudulent emails and online banking.

It is based on this knowledge and experience that I put forward this submission to the current review of the 2016 Census. The following document highlights my concerns about a number of aspects from the terms of reference as well as additional items for consideration by the committee. I welcome the opportunity to put forward these points for your consideration.

Should you wish to discuss further the content of this submission, please contact me directly on the details below.

Dr Cassandra Cross
Senior Lecturer, School of Justice, Faculty of Law, Queensland University of Technology

Publications: http://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

The following submission will address the following terms of reference:

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

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

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

j. any related matters.

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

The 2016 Census saw a marked shift in the way that the ABS attempted to administer the Census. In all previous Census collections, paper based forms were the primary way that individuals completed this task. The 2006 Census saw the introduction of the e-Census, which was an alternative available for households to complete. This continued in 2011 but was still an alternative to the paper based form (in 2011, approximately one third of all households completed the census online, a significant increase from 2006). In 2015, the ABS decided to change the procedure for the 2016 Census, with the e-Census format determined as the primary method of completing the Census. As a consequence, households were not mailed a form, but were instead issued with a notice that contained a unique code, which directed them to the ABS website and enabled them to complete the census online.

While the shift to the electronic completion of the Census in (and) of itself is not necessarily a bad thing (and beyond the scope of the current discussion), the Government failed in its responsibility to educate and inform Australian citizens about this significant change. There was a limited marketing and advertising campaign to educate citizens on the change to the way that the 2016 Census was to be completed, and this was highly inadequate in being able to effectively communicate the change in delivery methods. There was still an ability to request a paper-based form, however this required contacting the ABS by telephone to specifically request a form to one's household. It is well documented that the call centre was unable to cope with the demand (being volume of requests for paper-based forms), with many people unable to get through in a timely manner. If successful, there was then a further wait for the paper-based form to be delivered by Australia Post and for many households the requested paper form did not arrive until after the August 9 Census date.

It appears that the ABS made an incorrect assumption that given the current embracing of technology for everyday tasks, business and communication, that a transition to an e-Census would be simple. However, this assumption was inaccurate and proven to be an overestimation of society's ability and willingness to engage in an online environment, without sufficient information and preparation. In particular, the 2016 Census example highlights the need and importance of adequate public awareness campaigns which communicate clearly to individuals any changes to well

established processes. A large proportion of the uncertainty and confusion related to the shift from a paper-based form to an electronic form is likely to have derived from a lack of information about these changes and misinformation about the threat of fines for non or late completion. On such a large scale, it seems to be a significant oversight by the ABS and the Government to have not conducted a more comprehensive and lengthy campaign to educate citizens on the changes to the Census and how this would impact on individual households completing the form.

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

There are many individuals who are far more experienced and knowledgeable on the technical aspect of events which happened on Census night. Therefore, I am not in a position to comment on the operation of the website or its subsequent failure. However, the response provided to the public in the days after the events which took place on August 9 was unacceptable. Firstly, if the ABS did decide to take the Census website offline at 7:30pm on the night of the Census, then it should have communicated this honestly to members of the public who spent many wasted hours and efforts in attempting to complete the Census electronically, at the continued request of the ABS. The outright denial by the ABS of the issues which were being experienced caused delays and frustration to the public and undermined the trust of the public towards the ABS and the Census overall.

Second, the public messages delivered by members of the ABS and Government on Wednesday August 10 were inconsistent, speculative and unhelpful in seeking to reassure the Australian public about the safety and security of the Census data. Mr David Kalisch (ABS), Minister Michael McCormack, Prime Minister Malcolm Turnbull and Cybersecurity Advisor to the PM Mr Alastair Macgibbon all fronted the media with competing claims as to whether the incident was or wasn't a Distributed Denial of Service (DDoS) attack, whether it was or wasn't perpetrated by hackers, and finally, whether this attack/non-attack originated externally or internally to Australia. The inability of these key figures to present a clear and consistent message to the public on what happened triggered a wave of speculation as to what occurred and arguably, induced a large degree of anxiety and panic amongst citizens who had already completed the Census, or who were yet to complete. Further to this, despite ongoing claims that the site was subject to a DDoS attack, evidence was provided to media outlets which refuted these claims and added to the increased level of uncertainly that ensued. The backlash to the Census overall was captured on social media, through the Twitter hashtag #CensusFail, which at one point was the number one trending topic worldwide (at a time when the Rio 2016 Olympics were on). This in and of itself illustrates the extent to which concerns over the Census were evident and being communicated.

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

This particular term of reference is what I believe is at the core of the issues experienced by the 2016 Census. The changes to the 2016 Census significantly impact on the privacy of Australian citizens through the use of statistical linkage keys to combine Census data with other Government administrative data sets. The process undertaken by the ABS to consult on these proposed changes initially, the privacy impact assessment which was conducted, and the subsequent communication of

these changes to the public, were largely inadequate. The ABS first announced the intent to retain names and addresses in order to match these to other data sets in a press release issued on the 11 November 2015. This release stated that a privacy impact assessment would be undertaken and invited comments by 2 December 2015. In response to this, only two articles (here and here) were published by the media on the topic, and only three submissions were received by private citizens who all raised concerns with the proposal. Compared to previous privacy impact assessments, this one was conducted internally and not subject to the external agency review as witnessed in preceding years.

In addition, the ABS had contracted a market research company to undertake 16 focus groups with members of the public to gauge their sentiments towards the changes. The focus group research was generally favourable, though the report did identify a number of potential risks: Unauthorised non-ABS access to data stored in the ABS environment; Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation; Reduction in participation levels in ABS collections due to loss of public trust; and 'Function creep' – unintentional expanded future use of retained name and address information. Each of these risks was deemed "very low".

Consequently, the ABS put out a second media release on 18 December 2015, which announced the implementation of proposed changes to retain names and addresses in order to facilitate "a richer and dynamic statistical picture of Australia through the combination of Census data with other survey and administrative data" (ABS, 2015). This media release did not result in any known articles across the Australian media conveying the significance of this change to the Australian public.

The way that privacy concerns regarding the Census were dealt with by both the ABS and the Government, is what I believe to be the most disappointing aspect of the whole Census 2016 debacle (dramatic). The inability of the ABS to engage effectively with the public, experts, academics and other interested parties regarding the proposed changes as well as their inability to conduct an adequate privacy impact assessment which demonstrates a lack of understanding and concern over the potential implications for individual privacy enacted through the proposed changes.

The timing of both the public consultation and the release of the announcement were not ideal. There was limited media coverage and public engagement on these changes initially, as demonstrated through the receipt of only three private submissions to their inquiry. Based on events since the Census, it is clear that there is substantial public interest in these issues, and therefore suggests that there was not an adequate level of awareness to contribute a submission in the first place. Additionally, the use of market research is problematic as it engages a small group of people without necessarily the required knowledge or expertise to ask relevant and pertinent questions. The full report produced from this task can be accessed here.

The use of a statistical linkage key is of genuine concern with regards to the privacy and anonymity of Australian citizens. While the ABS has not specifically stated the type of linkage key to be used for Census data, the ABS website provides a link to the SLK581 linkage key, which is in use in other Government departments. This key uses a prescribed combination of letters and numbers from an individual's details and does not offer a high level of anonymity. While others are in a much stronger

position to discuss the problems with statistical linkage keys more broadly and their inability to afford anonymity to those involved, at minimum, the assurances of anonymity promised by the ABS in linking Census data to other data sets should be questioned.

Of major concern is the lack of consent gained by the ABS in implementing such fundamental changes to the Census data. Historically, Census data has been simply a count, and individuals have been content to provide names and addresses on the basis that these were destroyed within a set timeframe (18 months) and were only used to ensure the quality and accuracy of the data. The retaining of names and addresses for a longer period of time (4 years) and the creation of a statistical linkage key to be retained indefinitely, is a fundamental shift in the way that Census data has been used in the past.

As a researcher, I am governed by the National Statement on Ethical Conduct in Human Research. All work that I do which is related to human (including the use of data from administrative data sets) must be approved through an application process whereby as the researcher, I am responsible for demonstrating that I have considered how my work will impact on individual privacy and security, how I will maintain the wellbeing of my participants, and how I will gain informed consent from participants to use their data in a prescribed manner. It also requires me to be upfront with participants on the specifics of how their data will be used and whether I intend to use it for future projects and/or publications.

The changes to the Census which have been implemented around the creation of a statistical linkage key for indefinite use would be rejected outright by any ethics committee. There has been no effort on the part of the ABS to obtain informed consent from any citizens about the use of their data. There is no ability to opt out of the linkage and withdraw participation at any time without penalty. The Census is mandatory and compels all citizens to complete. There have been hollow assurances given by the ABS about the privacy and security concerns of citizens on the retention of their data. The National Statement is a critical document which governs the standard of research which is conducted across Australia in an effort to ensure that participants are not foreseeably harmed as a result of a research project. The standards that I and all of my academic colleagues are governed by, would not be met by the Census changes, with the inability of the ABS to provide the requisite information and evidence to support these guidelines. While I acknowledge that the operations and duties of the ABS are different to research conducted by universities, I believe that the principles surrounding informed consent and other target areas under the National Statement are valid in and of themselves and should be a standard ascribed to for research undertaken by agencies such as the ABS.

The failure of the ABS to meet many of the standards of the National Statement is problematic for a variety of reasons. The Census contains a comprehensive amount of data on Australian citizens and this data may be used to achieve a detrimental outcome against a person in the future. While there may be no reason to distrust the current Government and its intentions for using Census data (premised on an assumption of incompetence rather than malice), this is not a guarantee for future governments. Once the data is available, once it has been collected and once a linkage key has been created, it can be used for a variety of purposes, some of which may be detrimental to certain individuals or populations. This has a historical precedent, with Census data being used by

governments to identify minority groups within the population and subject them to abuse. There is historical evidence from World War Two that the USA used Census data to identify Japanese Americans and detain them in camps, as well as evidence to suggest that Germany used Census data to target Jews and other ethnic minorities. Given the current political and cultural climate, which can be argued as largely deriving from fear of "the other", it is not outside the realm of possibility to suggest that Australian Census data could be used for similarly objectionable actions in the future.

The linking of Census data to other data sets in and of itself may also pose distinct concerns for individuals (citizens). Rather than remaining at aggregate levels, the linking of data enables detailed pictures to be developed of individuals which may make them vulnerable to exploitation or extortion in the future, should there be a data breach. Documents obtained through the FOI process indicated that the ABS put forward a number of other datasets that could possibly be linked to Census data, as directly quoted below.

"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".

The linking of Census data to these other administrative data sets has the ability to paint a detailed picture of individuals and in and of itself, poses challenges to the privacy and anonymity of those subjected to it. In addition to the previously detailed concerns about consent and privacy, this quote also highlights the potential value of the data and the large array of areas that Census data could be linked to. It is therefore inevitable that these datasets will be seen as an attractive target (otherwise known as honeypot) for hackers and if compromised, could expose individuals to immeasurable and irreparable harm. There is no system that is "unhackable", including the ABS. A good security principle remains that if data is not collected, it cannot be hacked.

It is equally important to recognise that the threat of compromise or breach does not rest exclusively with the idea of an external "hacker". Rather, there is also the potential that a data breach could occur through the actions of an insider (employee) who may act out of negligence (for example, through the loss of a laptop, USB data storage device) or may act out of malice in leaking personal and damaging information. There are many examples of all types of data breaches which have occurred globally.

This section has canvassed in some detail, many of the privacy and security concerns which were relevant to the debate surrounding the changes to the 2016 Census. There are many valid points in these arguments which deserve acknowledgement and also deserve a response and consideration. However, in the events leading up to the 2016 Census and after Census night, both the ABS and the Government demonstrated a complete lack of understanding of the severity and legitimacy of these issues. This can be demonstrated in the following examples:

Minister Michael McCormack responded to concerns over the privacy aspects of Census, stating that the Census was no worse than Facebook. He likened the collection of Census data to that of supermarket loyalty cards and social media platforms such as Facebook and Twitter. The use of these comparisons are highly problematic. These are all voluntary schemes which individuals can opt-in or opt-out of. Users also have the ability to decide what type and extent of personal information is shared across a variety of security settings. There are also no fines involved for not participating in any of these schemes or platforms. Lastly, in my work and that of many others, there is an identified need to educate people about the level of personal information that they share wither willingly or inadvertently. Much cyber safety education is targeted at improving the security practices of people and restricting what degree of information is shared. This is a significant problem rather than a justification for the changes to the Census. Overall, this comparison demonstrates a complete lack of insight and understanding about the nature of the privacy and security concerns raised by citizens.

Minister Christopher Pyne accused parliamentary colleagues of engaging in "tinfoil hat politics" when several senators voiced their concerns about the 2016 Census. This comment intended to shut down the debate and discussion which was happening on the day of the Census but only served to demonstrate how those within the Government were still not taking any of the privacy and security concerns of members of the public and other politicians seriously.

The ABS advised the public that their site was "unhackable" and that there would be no future data breaches of Census data. It is both foolhardy and naïve to make these claims. As previously stated, no site or organization is immune from the potential of hackers. There are daily examples of systems and companies that have been exposed. Notable government examples include the citizenship database of Turkey being compromised, as well as the Office of Personnel Management (USA) and allegedly the National Security Agency (USA). The ABS itself has been the subject of 14 data breaches since 2013, and while none of them affected Census data, it and of itself this demonstrates that the ABS systems are not impenetrable. Any claim by an agency or government that a site or a system is "unhackable" is false and misleading to the public it is seeking to reassure.

There was also a strong focus by Census advocates who continually referred to the fact that names and addresses had previously been collected as part of the Census and therefore used this argument to discredit concerns about practices surrounding the 2016 Census. This is a valid point. However, this statement by itself does not seek to address the root of many concerns, which was not necessarily the collection of names and addresses in the first place, but the increased retention of these variables from 18 months to four years and the subsequent creation of a statistical linkage key for each individual based on these variables. These are two very different arguments and a focus on the first at the expense of engaging with the second, was not useful in the overall debate. The increased retention and use in linking data is a fundamental change to the way that Census data has been used and deserved to be acknowledged as such.

Overall, the Census is an important mechanism. Few people would argue against the merits of the Census and original intention of the data to support government decisions. This is reflected in the experience and successful completion of the Census in previous years. However, while the Census is arguably important, so too are the genuine concerns of citizens over their privacy. These two areas

should not be mutually exclusive and the desire to have one, should not automatically override the other. The events which occurred in the lead up to and after the 2016 Census, demonstrate that concerns of citizens about their privacy were minimized, trivialised and largely ignored by the ABS and the Government, rather than engaging in a constructive and honest conversation about the changes. It is on this basis that the ABS has likely lost the trust of many Australians and their confidence in the ability of the ABS to maintain the security of their data as well as privacy and anonymity concerns. Trust is hard to establish but very easy to lose, and the 2016 Census is likely to have lasting negative effects on what was a previously overwhelmingly positive relationship between the ABS and the community.

j. any related matters.

The above points deal primarily with the privacy and security concerns which were raised as part of the 2016 Census. However, there are a number of additional topics which are relevant and need to be considered in conjunction with any assessment of what occurred with the 2016 Census. These are:

1. Identity theft
2. Mandatory data breach reporting legislation
3. Human rights protections
4. Victim's voices

Each of these will be detailed in turn.

Identity theft

Identity theft is recognised as one of the fastest growing crimes of the current millennium. A report in 2015 indicated that 772,000 Australians were victims of identity theft in 2014. Additional statistics estimate the figure to be higher at 1.7 million. This type of crime poses increasing challenges for police as well as victims in seeking both to respond to known instances and prevent future instances from occurring. A person's identity credentials can be compromised in a number of ways, and includes actions of the individual as well as third party breaches. Regardless of how an identity is compromised, there can be substantial impacts for those affected in seeking to restore their identity.

I am currently involved in a research project with Dr David Lacey and partner organization iDcare. Our project seeks to map the experiences of victims in negotiating the "identity ecosystem" otherwise understood as the wide variety of agencies that victims must interact with in the aftermath of an identity credential being compromised and/or misused. While this research is ongoing, initial results from an analysis of 1526 case files indicate some important findings. In this data, we grouped victims into categories depending on how their identity was compromised in the first place. There are those who enabled the compromise (for example, those who respond to fraudulent emails with their bank account/credit card information), those who did not enable the compromise (for example, those who have been the victim of theft or third party data breaches (where a company they do business with has been compromised)), and those who were unaware of how their identity had been compromised. Of those who are unaware, it is likely that many of these were the subject of third party data breaches, and only became aware that their identity has been

compromised when they became aware that there was a misuse of their credentials (for example, through the loss of funds, credit transactions that were not theirs, or notification of a new loan). Of the 1525 case files, 48% had enabled their compromise, 30% had not enabled their compromise and 22% did not know the point of origin for their compromise. Of relevance and concern for the current inquiry, those who did not know how their identity was compromised exhibited greater levels of distress compared to those in the other two categories.

This has consequences in the current environment where Australia does not have mandatory data breach notification laws. As stated, In many of these circumstances, it is likely that those who were unaware of how their identity was compromised were victims of a third party data breach, whereby a company that they have done business with and who holds personal data about them, have had their systems compromised and customer details exposed. In some cases these companies may be unaware that this has occurred, but in other cases, the companies may be aware but are not mandated to report this breach to those affected.

The process of restoring one's identity in the aftermath of a breach, regardless of how it has been enabled, is fragmented and overwhelmingly negative for victims. Therefore, in the context of the ABS retaining data for a longer period of time and creating a statistical linkage key to facilitate more comprehensive datasets being compiled, poses several challenges in securing the data as well as ensuring privacy and anonymity for citizens. Identity theft can cause significant harm and distress and cause irreparable damage to individuals. It is also difficult to implement measures retrospectively once a compromise has been experienced. While some credentials can be reissued (for example, credit cards) and others can be changed (for example, bank account details) there are many other identity credentials which are static and cannot be changed. Therefore once these are exposed, the impacts and long term effects can be devastating.

Mandatory data breach notification reporting

As previously stated, Australia currently does not have any mandatory data breach notification reporting laws (though I believe there has been some progress with legislation being considered). In practice, this means that any organisation who is aware that their system has been compromised in some way (by external or internal factors) in not required to notify affected individuals about the extent of the compromise and what, if any, of their personal data has been exposed. There are instances where both government and private companies voluntarily go public with data breaches (for example, The Queensland Department of Education, Kmart and David Jones).

The consequences of a lack of mandatory reporting mean that individuals who are have their personal details exposed are not made aware of this incident and therefore are unable to monitor their accounts or take other steps to prevent potential misuse from occurring. Instead, if their data has been misused by offenders after being compromised, they will only realise this once offenders have made unauthorised transactions, opened up new accounts and lines of credit, or committed another unauthorised act in their name. The effects of this on an individual can be debilitating, with the onus then on the victim of identity theft to establish what has happened and seek to restore their identity and address any damage and harm which has been done.

In the context of the current discussion, if the ABS was subject to a breach of the Census data, they are not required to report this to the public or those who are involved. Therefore, claims by the ABS that it has never been hacked (regarding its Census data) are not actually able to be verified and any future breaches could remain confidential and unknown until victims are exposed. The lack of a mandatory data breach notification scheme does not assist the public overall in their confidence of the ABS and its ability to maintain the security of Census data into the future.

Human rights protections

In addition to the lack of mandatory data breach reporting laws in Australia, there are also limited human rights protections offered by current Australian law. The absence of a Bill of Rights within Australia means that many protections afforded to citizens are only captured in legislation, which can be repealed and reformed at the behest of the government of the day. This is relevant to the current discussions on the Census data, regarding the current legislative provisions of data use and security. While these may be in existence in 2016, there are no guarantees that a future government could repeal the current provisions and replace them with those which use the data in a different and objectionable way. The establishment of an Australian Bill of Rights would assist with giving citizens greater security across a number of areas, including those affected by the collection of Census data and its potential uses.

Victim's voices

Lastly, the discussion around the 2016 Census and concerns over privacy and security have largely ignored the voices of victims and those who could potentially be affected. As has been demonstrated above, the ABS and the Government have not engaged in a meaningful way with the genuine concerns which have been raised by individuals across a number of areas, predominantly focused on privacy and security. In my research with fraud and identity theft victims, I hear firsthand stories of individuals who have experienced some horrific events and who have experienced significant trauma as a result of the incident itself as well as the reporting experience in its aftermath. Australia currently has minimal support services in place to assist victims of fraud and identity theft to recover from their victimisation. Rather, there is a large level of victim blaming attributed to the individual themselves, and a lack of recognition about the harm they have endured. Many are isolated and experience high levels of stigma and shame associated with their victimisation.

In the context of the current Census discussion, it is imperative that the ABS and the Government demonstrate that they have considered worst case scenarios for data breaches of Census data. It is both foolhardy and naïve to think that it could never happen, and therefore both the ABS and the Government must demonstrate that it has thought through a variety of possible scenarios and have measures in place to deal with the ramifications of any security breach or data compromise. This should not be seen as causing unnecessary alarm, but rather should be viewed as responsible government in terms of preparation. If a data breach was to occur in today's environment, my research demonstrates the inability of government to respond effectively to the needs of victims and also highlights the inadequacy of current infrastructure to support victims, particularly fraud and identity theft (both which are relevant to Census data).

Conclusion

The above submission has canvassed my thoughts and observations on the events leading up to and in after the 2016 Census. Overall, it is clear that this Census was an abject failure (exemplified and reflected in the prevalence of the #CensusFail hashtag).

The Census is an important exercise for government and until 2016, the ABS and the Government had the overwhelming support and cooperation of Australian citizens in completing this task. However, the changes made to the 2016 Census, and the way in which they were implemented and communicated to the community, and how the ABS and the Government responded to the events of August 9, illustrate the undeniable collapse of this good will and trust on several levels.

In looking for any positives to arise from this event, it is clear that there is a need to have a large scale discussion on the bigger picture topics of privacy and security, which came into sharp focus during the unfolding of the 2016 Census. However, it is imperative that these discussions are informed and constructive, with the Government deliberately targeting input and expertise from a wide cross section of community members, academics and researchers, and private sector organisations (particularly those in information security and cyber security). It is clear that the 2016 Census failed to achieve this with any level of success. It is also vital that both the ABS and the Government acknowledge the concerns raised and refrain from dismissing them in the same manner as witnessed in recent months.

In moving forward, it is my hope that this review into the Census can identify areas for immediate action, which seek to address the concerns raised within this submission, as well as those evident in submissions tendered to the inquiry more broadly. The 2016 Census is an opportunity to reflect on how things ended up going so badly, as well as implement changes to ensure that these types of foreseeable errors do not occur again. There is less than five years to heal the wounds and damage done from the 2016 Census, and I hope that this is able to be achieved.

At a minimum I would suggest the following recommendations to be implemented immediately:

- A guarantee that no one who did not provide their name and address for the 2016 Census will not be fined for this action
- An amendment to the relevant legislation which explicitly states that the Census does not require names and addresses from citizens
- An amendment to the relevant legislation which prohibits the use of a statistical data linkage key (such as SLK581) being used to join various administrative data sets to the information obtained by the Census