Protecting 2021 Census Information

Patrick Fair
ASSOCIATES

Preface

The Australian Census of Population and Housing (Census) will be conducted in August 2021. Census night is on 10 August 2021. It will include an online option known as the Census Digital Service. The Australian Bureau of Statistics (ABS) has engaged PricewaterhouseCoopers (PwC) as the prime information technology (IT) service and security contractor for the Census.

The ABS has engaged Amazon Web Services (AWS) to provide cloud-based IT infrastructure to support the digital components of the Census. PwC is responsible for the design, build, implementation and maintenance of the IT solution. AWS is responsible for providing standard services which PwC has selected and advised are appropriate for the Census.

This paper aims to provide an overview of how the information collected from participants during the Census (Census Information) will be protected from unlawful access, interference, or loss. It also examines whether foreign governments can seek access to information held in Australia and describes the technical and legal barriers which prevent foreign governments from obtaining access to Census Information stored with AWS.

AWS provided funding to undertake this analysis and prepare this paper. The views expressed in the paper are my own and are based on my knowledge, experience and the information available to me at the time of publication.

Patrick Fair,
May 2021

Executive Summary

The security and confidentiality of Census Information is fundamental to securing the participation of the Australian population in the Census.

In 2021, the ABS will, for the first time, utilise public cloud computing technologies for collecting and storing Census Information by engaging the services of AWS. Census Information will be stored and processed for a period of time on infrastructure located in Australia that is owned and operated by AWS.

The confidentiality and security of Census Information held on AWS systems will be ensured by:

- Multiple levels of technical protections including encryption in transit and at rest, preventing it from being accessible to any third party.
- Strict legal obligations imposed by Statute. Census Information cannot be "divulged or communicated" except as permitted by the Census and Statistics Act 1905 (Census Act).[1] Census Information cannot be made available by order of a court or tribunal and must not be made available to an agency or any person (including any foreign government) except as part of the process of producing statistics pursuant to the Census Act.[2]
- Contractual obligations between AWS and the ABS.

Census Information will be encrypted by the ABS before it is stored with AWS. Without access to decryption keys (which will be held by the ABS), anyone seeking to access the Census Information will see a string of unintelligible cipher text that cannot be read by a human.

In the event Census Information were stored with AWS in an unencrypted form, a warrant issued by a government agency, including an agency of a foreign government, would need to survive the many legal restrictions imposed under Australian law, and in the case of a US authority, under US law.

Census Information stored in Australia with a US company would be protected by the principle of sovereign immunity. In delivering services for the ABS, AWS would be able to claim derivative sovereign immunity under US law. If Parliament passes the *Telecommunications Amendment (International Production Orders) Bill 2020*, and an Executive Agreement is negotiated between the US and Australia under the *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**), the Australian Government will have the ability to resist any warrant seeking access to Australian Government data.

In every case, provided the ABS encrypts the Census Information and holds the encryption keys, a warrant or subpoena for delivery of Census Information would likely fail at the threshold. This is because the body of cipher text (encrypted Census Information) cannot be associated with any information described in a warrant. The use of encryption technology would make it impossible for any party to deliver whatever might be specified in a warrant. This is the ultimate protection of Census Information.

Accordingly, Census Information held with AWS will be secure, highly protected, and not accessible by law enforcement authorities in Australia, the US, or any other country.

[1] Census and Statistics Act 1905 section 19
[2] Census and Statistics Act 1905 section 19A

What is the Census

The Census measures the number of people in Australia and collects information about certain characteristics of the Australian population according to those present in Australian households on Census night. Since 1961, the Census has been conducted by the ABS every five years. Participation in the Census is mandatory, but the ABS seeks "willing participation" from Australians. about 95% of households participate and it is expected about 75% will respond online in 2021.

The information collected includes the address of the household and the names of those present. Information about the individuals in a household may include sensitive information such as racial and ethnic origin, religion, and health information. Collected information is combined to provide a detailed snapshot of the economic, social, and cultural make-up of Australia. Statistics produced using Census Information are used by the public and private sectors to make decisions relating to, among other things, Constitutional matters, the allocation of the GST and federal financial grants, and economic investment decisions. Census Information is aggregated and de-identified before being made publicly available in published reports and, on the ABS website.

The importance of the security and privacy of the information collected in the Census was explained to the Australian Parliament in 2000, when then Minister for Financial Services and Regulation, Joe Hockey MP, explained:

> *Australia has a justifiably strong reputation for the quality of its census information, which provides the statistical foundation for decision-making by the public and private sectors. This reputation has been achieved, not only by the Australian Bureau of Statistics' sound work, but also by the public trust that the information collected will be protected. The government believes that nothing should be done which will put at risk public cooperation and hence the quality of census information.*[3]

The Security of Census Information

Census Information is protected by domestic laws and is not accessible to international authorities using domestic procedures. Census Information held by AWS is protected by contractual obligations and technology protections. Census Information that is encrypted using the tools, systems and services made available by AWS, will not be readable by any third parties, except where the ABS chooses to share the information or the encryption keys with those parties.

Technology Protections for Census Information

AWS's cloud computing services will enable the ABS to build technology solutions, including security solutions, to deliver the Census.

AWS will be providing its infrastructure and cloud computing services on the basis that the ABS is responsible for maintaining control over the content that is hosted on AWS infrastructure, and AWS is responsible for protecting the infrastructure that runs the AWS Cloud AWS will provide tools and guidance for the ABS to secure its data, and it will be the responsibility of the ABS (through its advisor PwC) to ensure the tools are used effectively.

[3] Hansard, Australian House of Representatives, Thursday, 17 February 2000 Page: 13724

AWS cloud services are secured and continuously monitored under globally recognised, and industry leading security assurance frameworks and certifications, including IRAP, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SOC 1, 2, and 3. These measures are validated by third-party assessors and are designed to protect customer data from unauthorised access. For example, ISO 27018 provides for protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to PII processed by public cloud service providers.

Using AWS tools and/or third-party tools, the ABS can ensure that only ABS employees or other authorised individuals can access comprehensible Census Information on AWS services. The ABS can encrypt Census Information at rest and in transit. If the only decryption keys are held by the ABS, third parties will not be able to read the Census Information.

Laws Protecting Census Information

Census Information is protected by several Australian laws and codes.

Census and Statistics Act 1905

Under the Census Act, the ABS is permitted to publish general statistical information but prevented from publishing "results or abstracts" that are "likely to enable the identification of a particular person or organisation."[4]

Privacy Act 1988

For the purposes of the Privacy Act 1988, the ABS is a body appointed for a public purpose by, or under a Commonwealth enactment, and therefore an "agency" within the meaning of the Privacy Act. Australian Privacy Principles 11.1 requires the ABS to take such steps as are reasonable in the circumstances to protect Census Information from misuse, interference, and loss, and from unauthorised access and modification.

The ABS has prepared a privacy policy specific to the 2021 Census.[5] The ABS is also subject to the mandatory data breach notification scheme within the Privacy Act, and AWS has offered an Australian notifiable data breach addendum to help the ABS comply with that scheme.

Freedom of Information Act 1982

The Freedom of Information Act 1982 (FOI Act) provides Australians with a general right of access to information held by Commonwealth agencies. Documents containing information collected under the Census Act are excluded from the FOI Act.

Archives Act 1983

Once Census Information is provided to the Australian Archives, it is protected by the Archives Act 1983 (Archives Act).

Criminal Code Act 1995

Under the Criminal Code Act 1995 (Criminal Code), criminal offences apply for unauthorised access to communications and stored information. Offences that help to protect Census Information in transit are expressed in the Criminal Code, Chapter 10, Part 10.6.

Offences that help to protect Census Information held at rest are expressed in the Criminal Code, Chapter 10, Part 10.7

[4] Section 12(2) of the Census and Statistics Act 1905
[5] 2021 Census Privacy Statement

> AWS does not have visibility into customer content and does not access or use customer content.

Contractual Obligations to protect Census Information

AWS provides customer access to its cloud computing services pursuant to contractual terms of supply. Clauses 3.2 and 3.3 of the AWS Customer Agreement state that:

- The customer may specify the AWS Region, which is the physical location of the cluster of data centres, in which content may be stored.
- Other than for specifically agreed reasons relating to the operation of a service or the fulfilment of legal obligations, AWS will not:
  - disclose content to any government or third party or
  - move content from AWS regions selected by the customer.

AWS has an Australian Data Privacy statement which summarises AWS's relationship to customer data as follows:

> *"Customers maintain ownership and control of their customer content and select which AWS services process, store and host their customer content. AWS does not have visibility into customer content and does not access or use customer content except to provide the AWS services selected by a customer or where required to comply with the law or binding legal order."*

[4] Section 12(2) of the Census and Statistics Act 1905
[5] 2021 Census Privacy Statement

Australian Government Access to Census Information

> *Given the statutory, contractual, and technical protections that exist to secure the Census Information, are there any circumstances in which Census Information could be accessed for purposes other than the delivery of the Census?*
>
> *For example, could an Australian law enforcement entity obtain access to the Census Information?*
>
> ***The answer is no.***

The usual means by which an Australian government agency, for a law enforcement purpose, would obtain access to information held by a third party (including an independent statutory agency like the ABS), is via an inter-agency request, or by order of a court or tribunal.

This is not the case for identifiable Census Information, which includes any information that is contained in a form that is given to the Statistician or an authorised officer. Sections 19, 19A, and 19B of the Census Act collectively prohibit this Census Information from being provided to any person, court, tribunal and or agency. Aggregate and de-identified information, in the form of statistics, and analysis arising from Census forms, is not protected.

By operation of section 19A of the Census Act, Census Information is protected from disclosure pursuant to warrants issued under the *Crimes Act 1917, Surveillance Devices Act 2004, the Telecommunications (Interception and Access) Act 1979*, and from the power of State and Commonwealth agencies to provide information and assistance under section 3LA of the *Crimes Act* and 64A of the *Surveillance Devices Act 2004*.

Similarly, Technical Assistance Requests (TAR), Technical Assistance Notices (TAN) and Technical Capability Notices (TCN) issued under Part 15 of the *Telecommunications Act 1997* could not be used to access Census Information.

Section 19A(1) of the Census Act, provides that the Statistician, or their officer, cannot be required to divulge Census Information to an agency (broadly defined) while, section 19A(2) of the Census Act provides that the Statistician, or their officer, cannot be required to divulge Census Information to a court or tribunal.

The Australian Crime Commission Act 2002 exempts information held under the Census Act from the power of the Criminal Intelligence Commission to obtain information held by an agency by service of a notice.

Apart from protection afforded by law, Census Information is also protected from disclosure by public interest immunity. In the case *The Australian Statistician v Leighton Contractors Pty Limited [2008]* WASCA34: 36 WAR83, the West Australian Court of Appeal prevented the lawyers of Leighton Contractors from having restricted access to name and address redacted survey forms collected by the ABS on the basis that the ABS is entitled to public interest immunity.

Foreign Government Access to Census Information

> *Is it possible that law enforcement agencies in another country, most particularly the US, could gain access to Census Information?*
>
> ***The answer is no.***

It is important to remember that where information is encrypted using available encryption tools, only the party holding the encryption keys - in this case the ABS - can decrypt the information. Without the information being decrypted, any warrant from any authority seeking access to Census Information would fail due to an inability to see the information in a human readable form.

Mutual Assistance

Generally speaking, the practical need for there to be international cooperation regarding the collection of evidence and enforcement of laws across national borders, is facilitated by bi-lateral treaties for Mutual Legal Assistance in Criminal Matters (MLAT).

Australia's compliance with its MLAT obligations is facilitated by the Mutual Assistance in Criminal Matters Act 1987 (MACMA). A foreign country can request the provision of material relevant to an investigation into, or proceedings in relation to, a serious offence against the law of the requesting country. Generally, the offence will be sufficiently serious if it relates to a criminal matter punishable by a maximum penalty of imprisonment for three years or more.

The MACMA gives the Australian Attorney-General various powers to act on MLAT requests.[6][7][8]

Australia's MLAT with the US was implemented in the *Mutual Assistance in Criminal Matters (United States of America) Regulations 1999*. Article 4 provides the Commonwealth Attorney-General the ability to deny a request that relates to a political offence, certain offences under military law, or those that would prejudice the security or essential interests of Australia.

Simply put, the Attorney-General would be entitled to decline any MLAT request for Census Information made by a foreign Government, including the US Government, on the basis that such a request would prejudice the essential interest of Australia having regard to a range of policy considerations including Australia's interest in maintaining public confidence in the Census.

It is highly improbable that Australia's Census Information would ever be relevant to proving a US criminal matter, and that AWS would be in possession of the Census Information in an unencrypted form, and that a US court would not recognise the protections given to Census Information by Australian law. In any event, the Attorney-General would still be entitled to decline any MLAT request for Census Information made by the US Government on the basis that such a request would prejudice the essential interest of Australia.

[6] section [15] of the MACMA
[7] section [15]B of the MACMA
[8] section [15]D(3) of MACMA

CLOUD Act provides mechanisms for the Australian Government and its US cloud service provider to resist any attempt to access Census Information

CLOUD Act

US law enforcement agencies have the ability to seek evidence held by providers of electronic communications or remote computing providers with a connection to the US,[9] even when the evidence is held outside of the US. Australian law provides similar powers to Australian law enforcement authorities. A US law enforcement agency would have to satisfy a US court that the evidence sought relates to a US crime, that there are sufficient facts to satisfy a court that there is probable cause to believe a crime has occurred, and that the evidence sought is directly related to that crime.

The CLOUD Act expressly preserved the ability of a cloud service provider to resist compliance to an order where compliance would breach a foreign law. This was done by inclusion in the CLOUD Act of a rule of construction preserving "the common law standards governing the availability or application of comity analysis."[10] In simple terms, this means the legal system of one country respects the laws of other countries.

In addition, where a country has a CLOUD Act Executive Agreement in place with the US government, a service provider issued with a warrant that applies to data held in that country may apply to a US court under §2703 (H)(2)(a) of the CLOUD Act to modify or quash the order if compliance "*would create a material risk that the provider would violate the laws of a qualifying foreign government*."[11] This would certainly be the case in relation to Census Information.

At the time of writing, an Executive Agreement under the CLOUD Act between Australia and the US is being negotiated. The Australian Government has published the Telecommunications Amendment (International Production Orders) Bill 2020 (IPO Bill), which would make changes to Australian domestic law to enable the Executive Agreement. Importantly in the IPO Bill there is no waiver of the provisions of the Census Act, nor any waiver of the sovereign right of the Australian government to protect government information. As a result, the passage of the IPO Bill would not adversely impact the ability of AWS and/or the Australian Government to resist a warrant under section 2703 of the CLOUD Act relating to Census Information.

In short the CLOUD Act provides mechanisms for the Australian Government and its US cloud service provider to resist any attempt to access Census Information.

[10] Note 103(c)
[11] https://www.law.cornell.edu/uscode/text/18/2703.

Sovereign Immunity

Sovereign immunity is a principle of international law, which applies in the US through the *Foreign Sovereign Immunity Act (FISA).* Its consequence is that "*… one state has no right to judge the actions of another by the standards of its national law. It protects an entity … by conferring immunity from adjudication (also known as immunity from suit) and by conferring immunity from enforcement and execution*."[12] FISA clearly states that "Subject to existing international agreements…a foreign state shall be immune from the jurisdiction of the courts of the United States…subject to certain exceptions for trading activities taking place within the United States."[13]

The concept of sovereign immunity extends to entities acting at the direction of the foreign state. This concept is known as derivative sovereign immunity, and US courts have recognised that derivative sovereign immunity covers contractors doing the work of a government. In delivering services for ABS, AWS be able to claim derivative sovereign immunity under US law for the ABS's benefit, to the extent that the AWS services involve executing a government function, namely, the ABS's collection management and use of Census Information.

Conclusion on Foreign Government Access to Census Information

The foregoing is a description of the legal framework that applies to cloud service providers, including AWS, and their obligation to provide Australian data pursuant to foreign government legal processes. In particular it considered how the US Government might seek access to Census Information.

It is most unlikely that a warrant would be issued against AWS for access to Census Information. If AWS were issued a warrant that required delivery of Census Information held in Australia, AWS could decline to comply with the warrant on the basis that the issuing court lacked jurisdiction, and AWS was entitled to derivative sovereign immunity.

For its part, AWS has publicly committed to acting to protect customers by challenging government requests for customer information. Given its available resources, the company would appear well placed to fulfil its commitment to "*challenge government requests for customer information that … are overbroad or otherwise inappropriate.*"[14] Most importantly, where compliance with a court order would put AWS in breach of Australian law, AWS can make a common law application to have the warrant set aside as a matter of discretion under the common law.

In every case, provided the ABS encrypts the Census Information and holds the encryption keys, a warrant for delivery of Census Information held by AWS would likely fail at the threshold. This is because the body of cipher text held by AWS (encrypted Census Information) cannot be associated with any information described in a warrant. The use of encryption technology would make it impossible for AWS to deliver whatever might be specified in a warrant. This is the ultimate protection of Census Information.

[12] https://www.ashurst.com/en/news-and-insights/legal-updates/state-immunity--an-overview/
[13] USC § 2604
[14] How does the Cloud Act impact AWS https://aws.amazon.com/compliance/cloud-act/

Glossary

Term	Meaning
ABS	Australian Bureau of Statistics
ACLD	Australian Census Longitudinal Dataset
Archives Act	Archives Act 1983
AWS	Amazon Web Services
Census Act	Census and Statistics Act 1905
Census Information	Information collected from participants in the 2021 Australian Census
CLOUD Act	US Clarifying Lawful Overseas Use of Data Act 2018
Criminal Code	Criminal Code Act 1995
DDoS	Distributed denial of service
FOI Act	Freedom of Information Act 1982
GST	Goods and Services Tax
IPO	International Production Order proposed by the Telecommunications Amendment (International Production Orders) Bill
IRAP	Information Security Registered Assessors Program operated by the Australian Cyber Security Centre
ISO	International Organization for Standardization based in Geneva Switzerland
ISO 27001	ISO/IEC 27001:2013 a standard published by the ISO specifying "the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organisation, including requirements for the assessment and treatment of information security risks tailored to the needs of the organisation."
ISO 27017	ISO/IEC 27017:2015 a standard published by the ISO providing "guidelines for information security controls applicable to the provision and use of cloud services by providing: - additional implementation guidance for relevant controls specified in ISO/IEC 27002; and - additional controls with implementation guidance that specifically relate to cloud services."
ISO 27018	ISO/IEC 27018:2019 a standard published by the ISO that "establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment."
IT	Information Technology
MADIP	Multi-Agency Data Integration Project
MACMA	Mutual Assistance in Criminal Matters Act 1987
MLAT	Mutual Legal Assistance in Criminal Matters Treaty
PCI DSS Level 1	The Payment Card Industry Data Security Standard, is an information security standard for organizations that handle branded credit cards from the major card schemes.
Privacy Act	Privacy Act 1988
PwC	PricewaterhouseCoopers
SOC 1, 2, and 3	Compliance audit reports based on standards issued by the American Institute of Certified Public Accountants.
US	United States
U.S.C	United States Code

About Patrick Fair

Professor Patrick Fair is the principal of Patrick Fair Associates, an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University, the Chairman of the Communications Security Reference Panel at the Communications Alliance. He is a member of the IoT Alliance of Australia Security Workstream and General Advisor to and an author of LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy. He was founder and Chair of the Internet Industry Associate of Australia and is a former President of the Law Society of NSW.