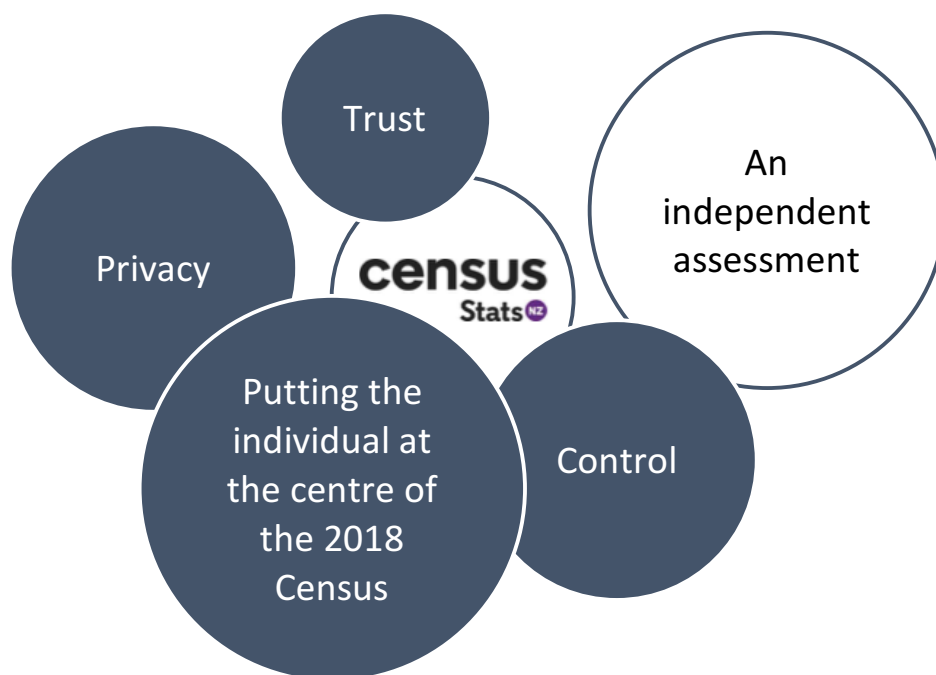

Simply Privacy.



2018 Census

Independent Privacy Impact Assessment
7 July 2017

By Daimhin Warner
Director (Auckland)
Simply Privacy Ltd

practical privacy solutions

Simply Privacy.

Table of contents

Key messages	3
Executive summary	4
Introduction	6
What is a PIA?	6
How was this PIA completed?	7
What is Simply Privacy?.....	7
2018 Census: Digital-first	8
The wider environment and context.....	10
Statistics Act: Providing a strong legal framework for census.....	10
Privacy Act: A roadmap for good privacy practice.....	10
Social licence: A privacy-supportive model	12
Current public perception: Is there social licence?	13
Culture, governance and technical security oversight	14
A strong privacy culture	14
Privacy governance structure and resourcing for census.....	14
Technical security as a wider issue	15
Collection: Ensuring value and managing risk	17
What information? A process to ensure value	17
Preliminary PIAs into census processes and systems	18
Practical privacy protections during the census	19
Data breach response plan	20
Use and processing: Limitations to increase control	22
Integration with the IDI	22
Stats NZ's access, de-identification and confidentiality processes.....	24
Openness and transparency: Communicating to build trust.....	26
Existing communications	26
2018 Census key messages	27
Where and how to deliver them.....	28
Conclusion.....	30
Appendix 1: Information gathering.....	31

Key messages



Executive summary

The census isn't just about data, or statistics, or intelligence. It's about people. It involves asking people to tell a government agency about themselves. It requires people to relinquish some control by entrusting often sensitive personal information to Stats NZ.

Stats NZ has expertise in data science. It can analyse, aggregate and extract insights from data with great skill but this assessment focuses on the extent to which Stats NZ recognises that this data is *about people* with privacy rights and expectations.

The assessment concludes that Stats NZ has a very clear picture of the person at the centre of the census. There is a strong culture of confidentiality within the organisation as a result of a well-established legislative framework that both facilitates personal information collection and use, and mandates a business model that treats personal information with care and respect. Stats NZ recognises the value of data as an asset and this informs its practices.

This assessment reviews the key processes, procedures and safeguards the census team has put in place, or is contemplating, to ensure that privacy remains a central theme in its planning and operations. The recommendations made in this assessment are aimed at ensuring that there is consistency between the census team and Stats NZ more generally, that privacy governance and oversight within the census team is sufficient and – most importantly – that the public knows about the good work being done to ensure that the 2018 Census is a privacy success.

The following recommendations are made:

1	Provide all census staff with guidance on the high level privacy goals and values for 2018 Census and build an understanding of the way each teams' processes, procedures and safeguards contribute to this.
2	Create and document clear privacy roles and accountabilities within the census team, including a central role with overall privacy responsibility.
3	Encourage close collaboration between this documented privacy role and Stats NZ's Privacy Officer and ensure the Privacy Officer has the opportunity to contribute effectively as 2018 Census processes are finalised.
4	Ensure that the census team reports regularly to the IPSaC Governance Group and that census privacy is a standing item on the Governance Group agenda.
5	Continuously revisit security safeguards as the census programme evolves, to ensure that they are facilitating good privacy practice.
6	Explain technical security safeguards to the public clearly and simply, to establish that the digital-first approach is good for privacy.
7	Revisit the decision not to undertake a full PIA on the EPIC processing system and consider rating the public impact of this system as high.

8	Ensure controls are in place to manage any perception that operational information incorporated into EPIC may be used for statistical or research purposes.
9	Link the census crisis communication approach to Stats NZ's wider incident management process and involve key privacy and security staff in the risk assessment, mitigation and notification stages of the process.
10	Notify the public that administrative data held in the Integrated Data Infrastructure ('IDI') will be used to improve the quality of census data and explain the overall value of this data use.
11	Notify the public that names and addresses are retained and used within the IDI's secure processing and linking environments to match information and explain the value of this data use.
12	Develop a clear and simple census privacy story that is structured to provide key privacy messages to the public and contribute to the building of social licence. ¹
13	Make the census privacy story easily accessible and stand alone and ensure that all channels connect to these key messages.
14	Tell the census privacy story well in advance of census, to build confidence in the digital-first approach and provide the time needed to revise communications to meet public needs or changing expectations.

¹ Social licence describes a level of public comfort with a particular use of personal information. This comfort comes from trust that personal information will be used only as promised and acceptance that enough value will be created by that use. It is discussed further below.

Introduction

This is an independent privacy impact assessment ('PIA') into the 2018 Census.

The census is a major public touchpoint for Stats NZ. It is a moment at which the agency engages extensively with the public and gathers personal information for statistical and research use. The census isn't just about data, or statistics, or intelligence. It's about people. It involves asking people to tell a government agency about themselves. It requires people to relinquish some control by entrusting often sensitive personal information to Stats NZ.

The 2018 Census is 'digital-first'. Unlike previous censuses, it will focus on digital engagement, encouraging respondents to complete the census online. This is positive for the NZ public. The digital-first approach (which also extends to the processing system and the management of workloads for field staff) is expected to reduce cost, increase engagement and deliver better information for research. However, these benefits cannot be achieved at the expense of individual privacy. Privacy must be built into the 2018 Census from the outset. This PIA is a part of that process.

Stats NZ has expertise in data science. It can analyse, aggregate and extract insights from data with great skill but this assessment focuses on the extent to which Stats NZ recognises that this data is *about people* with privacy rights and expectations. The assessment concludes that Stats NZ has a very clear picture of the person at the centre of the census and makes recommendations intended to ensure that this is demonstrated effectively to the public.

What is a PIA?

A PIA examines a change, project or proposal to evaluate how, and to what extent, it might impact on individual privacy. The PIA process is about designing privacy into changes, to ensure that risks are identified early and processes, products and safeguards are designed with privacy in mind from the outset. It's about setting the right course.

This assessment focuses on a number of key issues that are unique to the census. It does not confine itself to the Privacy Act or the information privacy principles but considers the 2018 Census within a wider context, taking into account the legislative framework, the current environment, public perception, and social licence themes. It is Stats NZ's intention to make this PIA available to the public. This is a commendable approach to take and shows a real commitment to accountability.

This is not a review of Stats NZ's technical information security. While information security is an important part of the overall privacy framework, it is a specialised part that requires separate and detailed consideration by information security experts. Stats NZ has engaged the services of Deloitte to assess these risks for the 2018 Census.

How was this PIA completed?

An independent PIA provides a fresh and impartial view over a process or set of processes that may have become business as usual to the agency itself. It is not affected by preconceptions or assumptions and should assist the agency to “see the wood for the trees”.

In undertaking this PIA, key census staff and teams were interviewed, with a view to understanding the governance structure, census processes, safeguards and controls either in place or contemplated. A significant document review has also been conducted, including internal process and policy documents, system outlines and diagrams, internal privacy impact assessments and external communications and other key materials.

A full list of interviews conducted and materials reviewed is attached at Appendix 1.

What is Simply Privacy?

Simply Privacy Ltd is a consultancy which provides privacy strategy, programme and consultancy services to public and private sector agencies. Simply Privacy’s directors have a combined 20 years’ of privacy experience, including in senior roles with the Office of the Privacy Commissioner, and have provided PIA and other assessment services to numerous agencies and on varied projects and processes.

In preparing this PIA, Simply Privacy has relied upon information, statements and representations provided to it by Stats NZ. Simply Privacy provides no warranty of completeness, accuracy or reliability in relation to this information, these statements or these representations.

2018 Census: Digital-first

At a high level, 2018 Census is no different from any other census and it is important for the public and stakeholders to appreciate this. Stats NZ has run censuses of the NZ public for decades. There is a general understanding by government and the public that censuses add value and are an important part of the process of government policy making.

Traditionally, censuses have been highly manual. Census staff have visited every home throughout the country to distribute and then collect paper census forms and return them to Stats NZ. The 2018 Census, however, will be primarily digital. Stats NZ will mail internet access codes to households and encourage the public to 'self-respond' online. The aim is for at least 70% of responses to be online. This digital-first approach is anticipated to improve data quality while reducing the cost of data collection.

As with previous censuses, census data will be integrated with other personal information held by Stats NZ in order to provide the statistics relied upon by the public and private sector to make sound policy decisions and drive better social and community outcomes.

The digital-first approach provides Stats NZ with opportunities to significantly improve privacy compliance, and the privacy experience of the public. A reliance on manual paper-based census processes created information security risks that can be very effectively mitigated in the online environment. Well-managed, the digital-first approach provides Stats NZ with a unique opportunity to better engage the public to show the value of census and build trust.

However, there are a number of changes to the collection and use of census data in 2018 that warrant specific mention and consideration here, not because these changes are inherently negative but because they are different and must be made clear to the public.

1. 2018 Census data is being collected in a different way. The flows of information that traditionally occurred will now be easier, faster and more efficient. Stats NZ is engaging a variety of third parties to facilitate these new data flows. Some of the questions asked in the census may also change, to reflect evolving priorities and attitudes.
2. 2018 Census data will be incorporated into Stats NZ's Integrated Data Infrastructure ('IDI'). The IDI is a database of de-identified personal information gathered from a wide range of information sources, including government agencies and NGOs. The IDI also contains the data from the 2013 Census.² For the 2018 Census, information will flow two ways:
 - IDI data will be used to improve the quality of 2018 Census responses, by filling gaps in responses and imputing data based upon clear links to other data already held.

² For a full list of IDI information sources, go to http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure/idi-data/idi-data-overview.aspx.

- 2018 Census data will be integrated into the IDI, and combined with other data collected, to provide a fuller dataset intended to drive better outcomes for New Zealanders.
3. To facilitate this integration, individual names and addresses will be retained within a secure IDI linking environment and used to more accurately link the 2018 Census data with 2013 Census data and personal information gathered from other sources. The retention and use of these identifiers may come as a surprise to the public and so is examined below in more detail.

These differences have the *potential* to impact negatively on the public perception of Stats NZ and on overall engagement with the census. If the public feel that the digital-first approach is facilitating a more intrusive, or less robust, census, they may be reluctant to provide good information on census day. If the public has a sense that the personal information they entrust to Stats NZ will be used in ways that make them uncomfortable, they may lose faith in the process.

The wider environment and context

Stats NZ operates in a unique context. It has a clear legislative mandate to collect a significant amount of often sensitive personal information. This mandate simplifies privacy considerations to some extent but in other ways it creates public perception issues unlike any other public sector agency faces.

Stats NZ must take particular care to display to the public that it is exercising its legislative mandate responsibly, fairly and in a way that is not overly intrusive. It requires Stats NZ not only to ensure that it has a lawful basis to gather and use personal information but also that its actions are measured and will add value and bring benefits to New Zealanders.

Statistics Act: Providing a strong legal framework for census

The Statistics Act gives Stats NZ legal authority to collect personal information of a certain type from individuals and it requires individuals to comply with such requests. This limits the application of the Privacy Act insofar as any actions are permitted by this legislative framework.

However, the Statistics Act also places a number of important obligations on Stats NZ and its staff that go above and beyond the more flexible obligations contained in the Privacy Act. It requires all staff to take a statutory declaration of secrecy in respect of the information they handle. It also places very robust information security obligations on Stats NZ, that are more onerous and comprehensive than the general requirements of the Privacy Act, and include an express limitation on the use of information (for statistical and research purposes only).

This legislative framework has influenced the culture within Stats NZ in ways that can have an impact on privacy practice. There is an overriding culture of confidentiality that informs the agency's processes and procedures. Provided that this culture does not result in complacency – and there is no evidence to suggest that it has – then this creates a highly safe and secure foundation for the development of sound personal information handling practices.

There is also a recognition – borne out in recent work by the Data Futures Partnership (and discussed in more detail below) – that the compulsory collection of personal information facilitated by the Statistics Act brings with it heightened obligations to be open and transparent.

Privacy Act: A roadmap for good privacy practice

While Stats NZ operates under a clear legislative mandate, it is still subject to the Privacy Act and the information privacy principles. The Privacy Act provides the safety net that ensures Stats NZ exercises its legislative mandate fairly, responsibly and in an open and transparent way. It has the flexibility to permit Stats NZ to operate in ways that are efficient and effective while supporting many of the safeguards the Statistics Act requires.

The Privacy Act requires Stats NZ to always ensure that it:

1	collects only the personal information it needs (for census, the information it is permitted to collect under section 24 of the Statistics Act);
2	collects personal information from the person concerned (for census, the respondent);
3	tells the public why it needs the information it has requested, what it will do with it, and who it may be shared with (for census, a major part of openness and transparency);
4	collects personal information in ways that are fair and lawful;
5	takes reasonable steps to keep personal information safe and secure (this is supported by section 37 of the Statistics Act);
6	enables individuals to access information about them;
7	enables individuals to correct their information if it is wrong;
8	takes reasonable steps to ensure that personal information is accurate before using it (for census, this includes steps to cleanse census data and ensure it is meaningful);
9	keeps personal information only for as long as it is needed;
10	uses personal information only for the purposes for which it was collected (for census, this is statistical and research purposes);
11	does not disclose personal information; and
12	takes care with unique identifiers.

While some of these principles apply less clearly in the Stats NZ context than others (for example, the access and correction principles are more difficult to comply with when significant steps are taken to de-identify personal information internally), they provide a set of foundational concepts that should inform general practice, particularly in respect of areas on which the Statistics Act is silent.

The Privacy Act and information privacy principles are also supported by the seven principles of *Privacy by Design*, which are intended to facilitate privacy practices that do not hinder the ultimate goals of the programme. For the census team, these principles are a relevant and useful set of reminders as the census draws near:

1. Privacy measures should be proactive not reactive;
2. Privacy should be the default setting;
3. Privacy should be embedded into design;
4. Aim for full functionality – positive sum;
5. Ensure end-to-end information security;
6. Promote visibility and transparency of risks and solutions; and
7. Make sure systems are user-centric.

Social licence: A privacy-supportive model

Where the collection of personal information is compulsory, issues of trust and control become more critical. While Stats NZ has a legislative mandate to collect and use this information, it needs to build an equivalent public mandate; a social licence to use information for the benefit of the community.

Social licence describes a level of public comfort with a particular use of personal information. This comfort comes from trust that personal information will be used only as promised and acceptance that enough value will be created by that use.

The Data Futures Partnership³ has identified a set of themes upon which it suggests that social licence can be built. These themes are components of transparency and they strongly mirror the information privacy principles.

Theme	How privacy supports this
Purpose <i>What will my information be used for?</i>	Collect only the information you need Tell people why you need it
Value <i>What are the benefits and to whom?</i>	Collect only the information you need Tell people why you need it
Use <i>Who will be using my information?</i>	Tell people why you need it Use it only for those purposes Limit access to those who need it
Control <i>Will my information be anonymous and could it be sold?</i>	Tell people who will have access to their information Ensure that it is protected Don't disclose it in an identifiable form Ensure that people can access their own information
Security <i>Is my information secure?</i>	Ensure that it is protected Ensure that it is accessed only for legitimate purposes Tell people about these steps

Using the information privacy principles and Privacy by Design principles as a benchmark for good personal information management, an agency can start to build social licence. Put another way, if an agency focuses on addressing the themes identified by the Data Futures Partnership, it will be less likely to fall foul of the Privacy Act.

³ For more information on social licence, and the work of the Data Futures Partnership, go to www.datafutures.co.nz.

Current public perception: Is there social licence?

Privacy is now an important public expectation. The media closely observes the personal information management practices of public and private sector agencies. Poor practices by other public sector agencies have negatively impacted upon public perceptions of the sector as a whole.

This creates challenges when attempting to build a social licence based on trust and control. Public perceptions measured in the years prior to the ACC privacy breach would likely have indicated a stronger social licence than exists today. High profile breaches – including the recent publicity around MSD’s demand for client level data from service providers – have shaken a general public assumption that personal information is in safe hands.

Further, the highly publicised failures during the 2016 Australian eCensus⁴ (known more colloquially as #CensusFail) may negatively impact on the NZ public’s perception of a digital-first census. The Australian experience may create caution among the NZ public that will need to be carefully managed. Stats NZ will benefit from the lessons learned from this incident, including the need to ensure that public communications are focused on the right privacy issues and are responsive and flexible.

Stats NZ has commissioned a number of surveys into public perception. A 2016 Colmar Brunton Use and Trust Survey⁵ focused on public understanding of the use of information and of trust in the statistics themselves. While the survey revealed a general acceptance that statistics are important, it gave no indication of any understanding of value as against individual privacy. The survey tested participants’ trust in the quality of the statistics Stats NZ released, not in Stats NZ as an agency.

A 2015 OPUS Survey on Public Attitudes to Data Integration⁶ came closer to measuring public trust in Stats NZ and its information uses. This survey showed some public discomfort with the idea that personal information may be held in a single database and linked to identifiers. Access, use and security were key concerns and participants indicated that they would find data integration more acceptable if they were persuaded that it was useful, fair, accurate, representative and in the public interest.

While these surveys show a moderate level of understanding and engagement from the public in the function of Stats NZ and, to some extent, the need for good statistics, they are some way off establishing the existence of any social licence.

As will be explained below, there is good reason to trust Stats NZ. However, in view of the more general perceptions of public sector privacy practice, it is suggested that Stats NZ should assume a low level of social licence and target its practices at developing openness and transparency to show value, build trust and start to earn one.

⁴ For a good outline of the eCensus failures and lessons learned, see Alistair MacGibbon’s *Review of the Events Surrounding the 2016 eCensus* 13 October 2016.

⁵ http://www.stats.govt.nz/about_us/what-we-do/our-publications/use-trust-in-oss-2016.aspx.

⁶ http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure/keep-data-safe/public-attitudes-data-integration-2015.aspx.



A strong privacy culture

As part of this assessment, a cross section of Stats NZ and census staff were interviewed. These interviews served two purposes. Firstly, they facilitated the gathering of important information about the 2018 Census processes and procedures. Secondly, they allowed for an evaluation of general privacy culture and values within both the census team and Stats NZ more widely.

Overall, it was very clear that Stats NZ has a strong culture of privacy and confidentiality, borne out of a legislative framework that focuses on security but also out of a general appreciation of the *value of data*. No person interviewed questioned the importance of privacy or an independent privacy impact assessment. All had an appreciation of privacy concepts and showed a strong understanding of privacy considerations that went beyond technical security safeguards.

It was also very clear that senior census staff grasped the importance of good privacy practice to the success of the census. As a result of lessons learned from Australia's eCensus, and due to the wider culture that exists within Stats NZ, senior staff have expressed a clear desire to ensure that privacy receives proper attention at the right time.

That said, the technical knowledge many staff showed in respect of the particular privacy and security processes in place within their functional unit (for example, census data collection, data processing, or the development of data products and services) appeared in some cases to cloud a more general understanding of the bigger Stats NZ picture. Some work may be required to tie these processes together and ensure that all census staff understand the end goal, which must be to provide the public with a simple value and trust picture.

Recommendation 1: Provide all census staff with guidance on the high level privacy goals and values for 2018 Census and build an understanding of the way each teams' processes, procedures and safeguards contribute to this.

Privacy governance structure and resourcing for census

Stats NZ has put effort into strengthening its strategic privacy oversight and governance.

As part of this, Stats NZ has established an Information Privacy, Security and Confidentiality ('IPSaC') Governance Group and Working Group. The Governance Group is executive level (members include the Chief Privacy Officer, Deputy Chief Executive – Data Services, Chief Methodologist, Chief Digital Officer and Legal Counsel) and it directs the Working Group (composed of senior staff including the Privacy Officer) to manage the development of the privacy strategy and programme. IPSaC minutes are shared with the Executive Leadership Team after each meeting.

Some organisation-wide privacy resource is available, though this is limited. Privacy is overseen by Organisation, Strategy and Performance which has a 0.6 full time equivalent dedicated resource (the Privacy Officer) to support the organisation's privacy practices. The privacy resource is small, particularly in view of the fact that Stats NZ is an organisation focused on the collection and use of information (including personal information). For this reason, the resource is limited in its ability to identify, manage and mitigate all privacy risks across the organisation.

This is made more challenging in relation to the 2018 Census because the census team is quite distinct from the rest of the organisation, with staff either engaged solely for this programme or seconded from other teams within the agency. This increases the risk of privacy gaps or weaknesses within census processes and makes it more difficult for Stats NZ's wider privacy resource to effectively ensure that privacy issues are being managed satisfactorily.

The census is particularly high risk from a privacy perspective and so it is important for the census team to ensure that privacy is adequately resourced, its internal privacy governance and accountability processes are strong and effective, and the team connects directly to Stats NZ's wider privacy risk and assurance processes. This should include sharing any preliminary PIAs (some of which are discussed below) with both the Privacy Officer and IPSaC Governance Group.

A real connection between the census team and Stats NZ's wider management of personal information will ensure consistency of approach and better oversight of privacy risks. It should also ensure that the many strong processes, procedures and safeguards being developed by various teams within census are consistent and clearly articulated to the public.

Recommendation 2: Create and document clear privacy roles and accountabilities within the census team, including a central role with overall privacy responsibility.

Recommendation 3: Encourage close collaboration between this documented privacy role and Stats NZ's Privacy Officer and ensure the Privacy Officer has the opportunity to contribute effectively as 2018 Census processes are finalised.

Recommendation 4: Ensure that the census team reports regularly to the IPSaC Governance Group and that census privacy is a standing item on the Governance Group agenda.

Technical security as a wider issue

Many of the risks presented by a 'digital-first' approach to the census relate to technical information security. The new information flows needed to facilitate digital engagement require the use of a range of technologies, platforms and information service providers. By outsourcing some functionality for the 2018 Census, Stats NZ is at risk of losing some control over the security of the personal information gathered.

Technical information security is an important part of the privacy framework. A mature agency has strong processes in place to ensure that the personal information it collects is safe

and secure at all times. This is not a technical information security assessment but it does seek to provide some assurance that Stats NZ is taking a proactive approach to information security as part of the 2018 Census development.

Stats NZ has engaged the services of Deloitte's Cyber, Privacy and Resilience team to provide independent advice and guidance on implementing a secure, vigilant and resilient approach for the 2018 Census. Deloitte has a wide mandate to assist Stats NZ and is delivering a broad range of ongoing advisory and support services in this regard, including systems review, incident response simulations, controls assessments, and advice on the procurement of third party information and technology related services.

For the purposes of this assessment, Stats NZ is taking more than reasonable steps to ensure that it builds security into the technology and systems it uses to run the 2018 Census. The recommendations below are intended simply to ensure that the security and privacy processes support one another and that the value these processes add is made clear to the public.

Recommendation 5: Continuously revisit security safeguards as the census programme evolves, to ensure that they are facilitating good privacy practice.

Recommendation 6: Explain technical security safeguards to the public clearly and simply, to establish that the digital-first approach is good for privacy.



The 2018 Census focuses on increasing public engagement, creating efficiencies, and also improving the quality of information gathered by Stats NZ. These are important and valid considerations that offer overall benefits to the community.

Further, the digital-first approach has the potential to better safeguard individual privacy than the previous manual approach. Online information gathering removes many of the risks inherent in paper-based processes. Today's technology allows for effective encryption of data at all points of the process and enables access controls to be put in place to manage use limitations.

As noted above, this is not an information security assessment. However, this assessment has touched upon the various steps, processes and systems the census team has put in place or is contemplating to safeguard personal information throughout the census information life cycle.

What information? A process to ensure value

The information Stats NZ is permitted to collect from the public is set out in the Statistics Act. Section 4 of the Act lists the classes of official statistics. Section 24 of the Act lists the particulars to be collected at census. The Government Statistician has a wide mandate to set the topics for any given census, provided that the information collected meets the requirements of section 4 of the Act.

Within these legislative boundaries, Stats NZ follows a careful process to ensure that any changes to the census are necessary and add value. The census must change from time to time to ensure that it is relevant and responsive to the particular conditions of the time. Otherwise, the information collected may not provide the insights needed to deliver important social and community benefits.

Stats NZ has developed a Content Determination Framework for this purpose. This framework includes public consultation and is designed to ensure that any new or altered census content is carefully considered. From a privacy perspective, this process is important because it:

- focuses on purpose and value, by requiring Stats NZ to establish the relevance of questions and the benefits these questions will deliver;
- encourages Stats NZ to exercise its legislative mandate responsibly and reasonably; and
- focuses Stats NZ on individual experience, by requiring a consideration of the impact a question might have on the respondent's impression of intrusiveness.

In the case of the 2018 Census, Stats NZ is coming to the end of the content determination process. It has applied the Content Determination Framework and is taking care to ensure that new content meets requirements.⁷

Preliminary PIAs into census processes and systems

As part of the census test conducted earlier in 2017, Stats NZ completed a number of internal preliminary PIAs with respect to individual processes, platforms or systems. These preliminary PIAs were intended to identify potential privacy risks early on. In each case, these assessments recommended whether a full PIA would be required.

The processes, platforms and systems assessed to date include:

1. Workload Creation and Allocation Tool (*using a tool to create and allocate work during address canvassing*)
2. Respondent Facing Contact Centre (*using a third party service provider to manage an expected increase in contacts from census respondents*)
3. Contact Centre Homeworkers (*using a mixed on and off site worker model for contact centre operations*)
4. EPIC system for census processing (*using software, tools and systems provided by EPIC for processing census data*)
5. Internet Collection System (*using a third party service provider to manage the collection and storage of online census responses*)
6. Census Onboarding (*managing the recruitment and day-to-day operations of census field staff*)
7. Post-Enumeration Survey (*collecting personal information after census to measure the accuracy of people and dwelling counts*)
8. Census Test Information Website (*creating a separate census.govt.nz website*)

For the most part, these preliminary assessments are comprehensive and well-considered. They follow a good structure, which ensures that key information flows are mapped and risks assessed. Stats NZ has explained that these are living documents. They will inform the development of final 2018 Census processes, platforms and systems, and will be amended as required to ensure that they remain up to date and relevant.

This is a positive step to take, and is evidence of the census team's overall concern about privacy and security (as noted above). The census team must ensure, however, that these preliminary assessments are consistently shared with the Privacy Officer and IPSaC Governance Group, and are not treated solely as a compliance exercise.

⁷ For more information on the status of the 2018 Census content review, go to <http://www.stats.govt.nz/Census/2018-census/prelim-content.aspx>.

Specific comments on preliminary PIAs

The **EPIC processing system** will collate and process census data (that is, the personal information people provide in their census responses) and so is a major part of 2018 Census delivery. The following comments are made about the preliminary PIA:

- The PIA notes that operational information about dwelling occupancy and respondent behavior will be incorporated into EPIC to assist with determining census completion. However, as noted below, the census team stated during interview that this operational information would be stored only in the CRM system and not integrated with any other information systems. This apparent inconsistency should be investigated to ensure it raises no risks – or public perception – of inappropriate use.
- The PIA rated public impact as medium. However, due to inherent sensitivities around the move to a digital-first census, and the importance of the information processing system to the security, accuracy and ultimate use of census information, it is recommended that public impact be rated as high.
- Overall, the PIA rated risks as either medium or high but recommended that a full PIA was not required. It is recommended that such a risk rating would warrant the completion of a full PIA in respect of the system, particular in view of the potential public impact of poorly managed risks.

Recommendation 7: Revisit the decision not to undertake a full PIA on the EPIC processing system and consider rating the public impact of this system as high.

Recommendation 8: Ensure controls are in place to manage any perception that operational information incorporated into EPIC may be used for statistical or research purposes.

The **Post-Enumeration Survey ('PES')** PIA rightly highlighted the risk that information about census completion might be used for purposes other than measuring census coverage. This preliminary PIA has suggested that any uses of PES information that go beyond measuring census coverage must be subject to a further PIA. This suggestion is supported.

The **Internet Collection System ('ICS')** is a major part of 2018 Census delivery. As with the processing system, a failure in the ICS during the census could have a major impact on public confidence (noting, for example, the Australian eCensus experience). The preliminary PIA into the ICS rightly identified public impact as high but recommended that a full PIA was not required. On balance, this outcome is supported on the basis that the major risks presented by the ICS relate to the security and integrity of the system, rather than the way personal information is used. The ICS service provider has outlined to Stats NZ the measures it will take to ensure that ICS security requirements will be met.

Practical privacy protections during the census

As with previous censuses, temporary field staff are engaged to manage the practical information gathering process before, during and after the census. The digital-first approach means less staff will be required in 2018. However, the 2018 Census will still require the

collection, retention and use of personal information about dwelling occupants in order to manage the process.

This information is distinct from the census responses and so raises different privacy issues. Information could include reports about occupant behaviour or safety concerns that may impact on other field officers or affect decisions about soliciting responses from a particular dwelling.

The census team has taken the following steps with respect to this part of the process:

- Field officers use tablets to record information about dwellings and occupants. These tablets are password protected.
- Operational information is retained in a CRM system and is not integrated with statistical information nor used by Stats NZ for statistical or research purposes (although, note recommendation 8 above).
- Where possible, field officers are not provided with individual names. Rather, the process is operated at the dwelling level. Incidents or concerns with a particular dwelling tend not to be linked to a particular individual.
- Field officers are provided with face-to-face and online privacy training to ensure that they understand Stats NZ's wider privacy expectations.
- Field officers are required to sign a declaration of secrecy.

These are positive steps, which taken together should effectively mitigate many of the privacy risks created by a large scale information gathering exercise such as census.

Having a presence in the field also provides Stats NZ with a unique opportunity to engage with respondents and reiterate privacy and trust messages. As will be discussed in more detail below, it is critical that field officers are equipped to do this in a consistent and meaningful way.

Data breach response plan

The 2016 Australian eCensus is a good reminder that things can go wrong. It is impossible to entirely negate the risk of data breach and it would be unreasonable to expect an agency to do so. For this reason, it is critical for Stats NZ to have a strong data breach management plan in place before, during and after the census, that includes clear escalation paths, reporting and communications processes.

Stats NZ has developed an agency-wide incident management plan that directs how staff should report and manage a security, privacy or confidentiality incident, or a near miss. The plan sets out an escalation path and guides staff through a process of reporting, containment and notification. The plan also ensures that a number of governance layers are involved in the management of the incident.

- **Staff** – Attempt immediate containment of the incident and report to security and privacy staff and their manager.

- **Manager** – Immediately review the incident and determine if further containment is required. Ensure incident has been recorded in incident log.
- **Security and Privacy** – Act as first point of contact and advise business. Evaluate level of risk. Start prevention process.
- **Triage team** – Assist with determining notification and communications, including to affected individuals, National Cyber Security Centre and Privacy Commissioner.

The census team recognises that strong communication is a critical part of managing a data breach. The team has developed a Crisis Communications Approach designed to ensure that any crisis – relating to people, systems or data – is managed quickly and openly. The team has taken a centralised approach, to ensure that any response is targeted and coordinated. It identifies three key phases:

- **Alert** – Senior Manager, Communications and Marketing. Crisis communications team will then schedule a meeting to begin managing the crisis.
- **Gather** – Relevant information to confirm situation and timeframes for response.
- **Respond** – coordinated communications will be developed, reviewed and adjusted as required, until the crisis is resolved.

It is very sensible to ensure that the 2018 Census takes a consistent and coordinated approach to managing a data breach. As we have learned from the Australian eCensus failures, communication is a critical part of an effective data breach response plan. However, the Crisis Communications Approach focuses only on this part of the process.

It will be important to ensure that the 2018 Census data breach response plan links clearly and effectively to Stats NZ's wider incident management process. Once a crisis, or incident, has been identified as involving personal information, it is important that privacy and security staff are involved and have input into the decision to notify (or not) and the nature of the communications that follow this decision.

A central theme of this assessment is the need to put the individual at the heart of census processes. The data breach response plan must reflect this too. Stats NZ's wider incident management process ensures that the right stakeholders are notified. These stakeholders can assist the census team to focus on the individuals and effectively assess the likelihood of harm. They can also assist the census team to take effective steps to mitigate harm and manage any negative public perceptions caused by a breach.

***Recommendation 9:** Link the census crisis communication approach to Stats NZ's wider incident management process and involve key privacy and security staff in the risk assessment, mitigation and notification stages of the process.*



2018 Census data forms a small part of the personal information Stats NZ routinely collects for statistical and research purposes. Census data is used by the agency in various ways to develop better statistical products that can deliver meaningful insights to drive better social and community outcomes.⁸

A key part of Stats NZ's overall privacy and security framework is its ability to effectively ensure that the personal information it collects – including census data – is accessed and used only for legitimate statistical and research purposes. Getting this right is critical to building trust and ensuring that the public has some sense of control over the way their personal information will be used and protected.

Stats NZ excels in this area. It has developed agency-wide processes to ensure that personal information is de-identified before it is accessed and used. Recognising that even de-identified personal information can identify individuals in some circumstances, Stats NZ takes further steps to “confidentialise” personal information before it is incorporated into statistical products or aggregated to provide statistical insights.

In addition, Stats NZ's systems and platforms include complex access controls that ensure only staff who need to see personal information before it is de-identified can do so. These processing and linking environments provide a safe platform for effectively linking the various datasets used to create statistical products and insights.

These processes go to the heart of Stats NZ's operations. They are elaborate and intelligent processes run by data scientists with expertise in understanding how best to ensure that risks of re-identification and unauthorised access are minimised.

Integration with the IDI

The IDI was introduced briefly above. Put simply, it is a database designed to facilitate effective data integration. The IDI pulls together a series of de-identified datasets from government agencies and NGOs⁹ (this data is referred to as “administrative information”) and integrates these datasets with census data from 2013 and, shortly, the data collected in 2018. Researchers can then apply to access the de-identified data in the IDI, under strict conditions outlined below, for statistical and research purposes.

While integration with the IDI is not the only use to which 2018 Census data will be put,¹⁰ it is a significant one. Data integration is viewed with some caution by the public, as noted above. Without strong controls around information linking, access and use, data integration

⁸ For examples of the products and services Stats NZ developed with 2013 Census data, go to <http://www.stats.govt.nz/Census/2013-census.aspx>.

⁹ For a full list of IDI information sources, go to http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure/idi-data/idi-data-overview.aspx.

¹⁰ See note 8, above.

could present significant privacy risks, particularly if identifiable information about individuals was accessible to the public or to other government departments.

Stats NZ's IDI team has approached data integration with care and consideration. Data Integration Guidelines,¹¹ which include a set of data integration principles (public benefit, use limitation, openness, and no integration where a promise has been made not to), have informed all IDI risk assessments. A number of complex PIAs have been completed into the IDI generally and as each new dataset has been considered for inclusion in the IDI. These PIAs are all publicly available.¹²

Integration for processing census data

Stats NZ is building a new infrastructure for the processing of 2018 Census data (referred to above as the EPIC processing system). In many respects, the processing of census data will be similar to previous censuses. The information security considerations with respect to this system are beyond the scope of this assessment and are, in any event, being addressed elsewhere.

However, the new infrastructure does facilitate a new use of personal information already held by Stats NZ, for the purpose of improving the quality of 2018 Census data. The processing system will link to the IDI and use administrative information to improve the overall input from the census. The system fills gaps in census responses and cleanses information collected during the census.

Section 37(1) of the Statistics Act states that information provided to Stats NZ can only be used for statistical purposes. Principle 10 of the Privacy Act takes a similar approach. It states that personal information should only be used for the purposes for which it was collected. Here, Stats NZ is proposing to use administrative information collected from government departments to improve 2018 Census data. This is being done for the purpose of improving the quality and linking of census data, and for the ultimate purpose of providing better statistical insights and research outcomes.

The proposed improvements are, therefore, consistent with Stats NZ's overall purposes and with the limitation contained in its own Act. However, this change may nonetheless come as a surprise to the public. For this reason, it is recommended that this change be explained clearly to the public in any privacy messaging created for the census. This recommendation will be revisited below.

Recommendation 10: Notify the public that administrative data held in the Integrated Data Infrastructure ('IDI') will be used to improve the quality of census data and explain the overall value of this data use.

¹¹ <http://www.stats.govt.nz/about-us/legisln-policies-protocols/data-integration-gdlns.aspx>.

¹² For a full list of the IDI PIAs, go to <http://www.stats.govt.nz/browse-for-stats/snapshots-of-nz/integrated-data-infrastructure/keep-data-safe/privacy-impact-assessments.aspx>.

Integration for developing better statistics

2018 Census data will also be integrated into the IDI and linked with 2013 Census data and administrative information datasets. It is clear that such integration also fits within Stats NZ's overall use limitations. The purpose of this integration is to improve Stats NZ's ability to develop meaningful and relevant statistical products and insights. The value is easy to understand.

However, to effectively link the 2018 Census data with information already held in the IDI, Stats NZ must retain and use a number of identifiers. In particular, Stats NZ proposes to retain individual names and addresses to match information within the IDI. This is not new. Names and addresses have been used within the IDI for some time to ensure that the information is accurate.

The Privacy Act permits an agency to retain personal information for as long as it is needed for a lawful purpose. Both the Privacy Act and the Statistics Act permit the retention and use of names and addresses to facilitate Stats NZ's wider purposes.

However, this may impact on public perceptions of census anonymity and control. It is important therefore to clarify that names and addresses are only used within the processing and linking environments. Stats NZ processes (which are outlined below) ensure that it is not possible for statistical products to reveal personal information that might identify a particular individual.

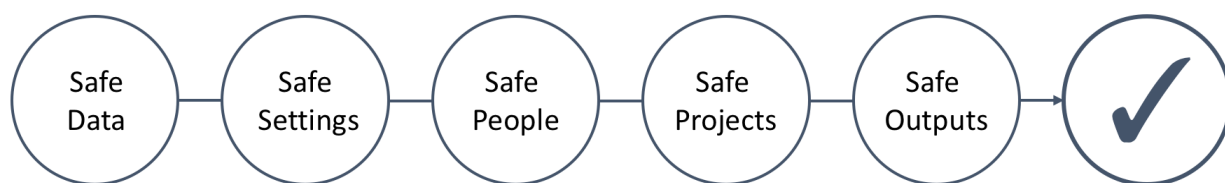
It is recommended that the retention and use of names and addresses within the secure processing and linking environments be made clear to the public at the outset. This recommendation will be revisited below.

***Recommendation 11:** Notify the public that names and addresses are retained and used within the IDI's secure processing and linking environments to match information and explain the value of this data use.*

Stats NZ's access, de-identification and confidentiality processes

Stats NZ's core operational model is focused on responsible and legitimate access to and use of personal information. The processes it uses ensure that the risk of identification of individuals is minimised while permitting the effective analysis, aggregation and use of personal information for statistical and research purposes.

Stats NZ achieves this by applying the **5 safes** framework. This framework is supported by technical security safeguards and audit and assurance processes to ensure that it is adhered to.



1. **Safe data** – Personal information is **de-identified** by removal of all unencrypted unique identifiers and identifiable information such as names and date of birth.¹³
2. **Safe settings** – Only staff who need to see identifiable personal information for processing or linking purposes have access to secure linking environments. Once de-identified, personal information can only be accessed by researchers through a secure Data Lab. Researchers can only access information relevant to their research.
3. **Safe people** – Those accessing personal information must sign a declaration of secrecy and pass reference checks. Researchers must also sign a research undertaking and understand and follow Stats NZ's rules and protocols.
4. **Safe projects** – To access the IDI, researchers must establish that their projects have a statistical purpose and are in the public interest.
5. **Safe outputs** – Personal information is further "**confidentialised**". Before being disclosed to the public (that is, outside the IDI and Data Lab environment) as part of Stats NZ's wider products, the statistical outputs must be run through a further process to ensure that individuals cannot be identified from the information.

Stats NZ's processes allow for the *controlled release* of de-identified information within a secure and carefully protected research environment, and the *public release* of confidentialised information. As the settings, people and project controls are reduced, the safeguards around the data itself are increased, thereby permitting a wider audience to benefit from statistical insights.

These processes effectively ensure that personal information gathered by Stats NZ – whether from a census or from another source – is protected. They allow Stats NZ to provide meaningful reassurances to the public that personal information is accessed and used only for legitimate statistical and research purposes. It is to this topic, to openness and transparency, that the assessment now turns.

¹³ For more information about Stats NZ's de-identification process, go to http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/integrated-data-infrastructure/idi-data/de-identified-data.aspx.



Openness and transparency has been a prevailing theme in this assessment. Stats NZ has developed very strong and sound processes and controls to protect personal information but these are not going to build trust if they are not known to the people they are intended to protect.

The census privacy story is about more than compliance with the Privacy Act. This is Stats NZ's opportunity to manage public perception and quell any misunderstandings about the way personal information collected during the census is used. It is an opportunity to tell the public that there are legitimate and valuable reasons for using personal information to better link and improve statistics. It is the opportunity to show value.

Stats NZ embraces transparency about its practices. Its willingness to make policies, processes, risk assessments and other key privacy materials public sets it apart from other public and private sector organisations and sets a benchmark for others to follow.

Stats NZ's website contains a wealth of information about the way Stats NZ manages personal information, from its governance structure and high level privacy policy and expectations to its complex physical, technical and procedural safeguards for ensuring that personal information is protected. There is a significant amount of detailed information available to the public, should they wish to access it.

Existing communications

The Stats NZ website provides the public with access to information about its general privacy policies and procedures,¹⁴ and the privacy and security steps in place with respect to the IDI.¹⁵

Privacy general – Stats NZ provides individuals with an overview of its approach to privacy compliance, along with detailed policy documents that outline in depth the privacy, security and confidentiality processes. The overview is plain English and clear. However, as noted above, this information is general and has wide application.

IDI – Similarly, Stats NZ provides specific privacy messaging in respect of the IDI, recognising that data integration raises particular concerns for the public. As with the general privacy content, an overview of IDI privacy and security is given, along with more detailed links to processes and procedures, including the de-identification and confidentiality processes.

The wider IDI content also includes an explanation of the datasets involved and the value they add. It should be noted that the messaging frames privacy primarily in terms of information security ("How we keep IDI data safe"). It is suggested that the datasets collected and the value these add should also be framed as key privacy messages.

¹⁴ <http://www.stats.govt.nz/about-us/legisln-policies-protocols/confidentiality-of-info-supplied-to-snz.aspx>.

¹⁵ <http://www.stats.govt.nz/browse-for-stats/snapshots-of-nz/integrated-data-infrastructure/keep-data-safe.aspx>.

2018 Census - At this point, no information has been provided to the public in respect of the 2018 Census privacy processes and procedures, in large part because many of these are still in development.

The census team did develop a set of privacy messages as part of the 2017 census test. These provide a good starting point to develop a census privacy story but should be complemented by something more holistic which focuses on the full information life cycle. It should be noted that these messages are focused largely on technical security issues and do not provide an overall value and trust message.

2018 Census key messages

During the census, Stats NZ targets every New Zealander. All people are asked to engage with Stats NZ at this point, regardless of knowledge, literacy or sophistication of privacy awareness. Being requested to provide detailed personal information to a government agency can make people feel uncomfortable and it is unlikely most individuals will take the time to study Stats NZ's website to find the information they need to get a full understanding of the census information life cycle and the reasons they should trust Stats NZ at census time.

For this reason, it is critical that the census team develops a **census privacy story** that is clear and simple and aimed at the wider population, not just those with the capacity, knowledge and understanding to engage with detailed technical documents. This story should:

1. be clearly census-focused but **branded** in a way that connects directly with Stats NZ;
2. very simply outline the **census information life cycle**, from collection online or in hard copy through to sharing either within IDI or as part of other products or insights;
3. provide a **compelling value proposition** to ensure that people quickly understand why they should provide their information and how this will benefit the community;
4. provide **clear notice** to the public about key issues that may impact on public perception, including the retention and use of names and addresses and integration with the IDI and explain that this is legitimate and adds value;
5. promote the **privacy and security benefits of a digital census** and provide quick and simple reassurances in respect of technical security standards in place;
6. show **transparency about the use of third party** information service providers, including cloud service providers, and link to any risks assessments undertaken into these providers; and
7. very simply outline the internal processes in place to ensure that **access and use limitations** can be trusted.

These messages support the themes that have been identified as critical to building social licence. It is in this openness and transparency space that Stats NZ can effectively start to create and build a public mandate for census, data integration and the work of Stats NZ more generally.

It is suggested therefore that the census privacy messaging be structured in a way that meets both privacy compliance and social licence goals:

Social licence themes	Privacy messaging
Purpose and Value <i>Why is my information being collected, and who does this collection benefit?</i>	What personal information is being collected? Why is this information important to Stats NZ, and to New Zealand more generally? What value will be added by data integration? What value will be added by retaining names and addresses?
Use and control <i>Who will be accessing and using my information and in what ways?</i>	Who will have access to the information, and in what forms? How will the information be used, and how will Stats NZ ensure that this is always the case? What will not happen with the information?
Security <i>Is my information secure?</i>	How is information protected during the census? How is information protected within Stats NZ? How are physical and process safeguards bolstered by technical safeguards? What will happen if there is a data breach?

Recommendation 12: Develop a clear and simple census privacy story that is structured to provide key privacy messages to the public and contribute to the building of social licence.

Where and how to deliver them

Simplicity and consistency are key to delivering one clear message to the public about the 2018 Census. People should be directed to one place to be provided with the key messages they need to feel comfortable. The publication of detailed process documents, PIAs or other technical information, while commendable, will not achieve this purpose and risks confusing the public and obscuring the key messages they need to understand.

It is recommended that the census team should aim to tell one story, in one place, that leads respondents through the key messages of purpose and value, use and control, and security. This story can link to more detailed technical documents, whether processes, procedures or PIAs, but should stand alone and give respondents enough information to understand and trust the process.

All census channels – whether field staff, contact centre staff or online content – should talk from the same simple script.

It is also recommended that this privacy story be told well in advance of the census. This will give the team the time needed to build confidence and revise its communications plans to ensure that the public's needs are met. By the time of the census, the benefits of a digital-first approach should be accepted.

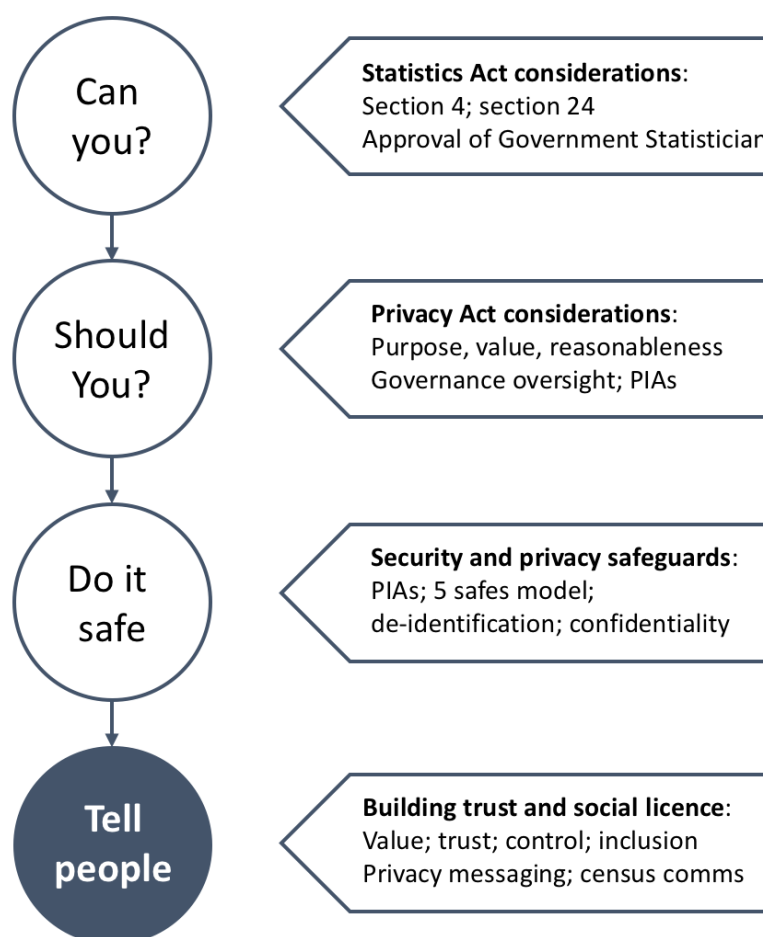
Recommendation 13: Make the census privacy story easily accessible and stand alone and ensure that all channels connect to these key messages.

Recommendation 14: Tell the census privacy story well in advance of census, to build confidence in the digital-first approach and provide the time needed to revise communications to meet public needs or changing expectations.

Conclusion

The 2018 Census is in good hands. The essential ingredients are in place to ensure that the 2018 Census can maximise the benefits of digital engagement and extract real value from data while recognising the person at the centre of it all. By taking a few steps to make sure that the many census processes and procedures link effectively with Stats NZ's wider privacy framework, the census team can meaningfully and honestly tell the public their personal information is in safe hands.

This census privacy story is key to building trust and confidence in the 2018 Census and in Stats NZ more widely. People need to understand and accept that concerns about value, use, control and security are recognised and taken care of. This story must demonstrate to the public that Stats NZ has considered whether it *can* collect personal information, considered whether it *should* collect personal information, ensured information collection and use can be *done safely*, and been as *open and transparent* as it can with the public.



With an understanding of the value of personal information and a clear picture of the ways Stats NZ ensures this information is used only for the benefit of the community, the public can and will wholeheartedly engage in the census process.

Appendix 1: Information gathering

The following individuals were interviewed as part of this PIA:

- Teresa Dickinson, Deputy Government Statistician, Insights and Statistics
- Denise McGregor, General Manager 2018 Census
- Richard Stokes, Senior Manager, Communications and Marketing (2018 Census)
- Nancy Linton, Senior Adviser Communications (2018 Census)
- Sarah Johnson, Manager, Census Programme Design and Integration
- Lyndsey Whelan, Manager, 2018 Census Processing and Evaluations
- Giles Reid, Senior Analyst, Processing and Evaluations
- Rory Sarten, Statistical Analyst, Processing and Evaluations
- Alan Bailey, Senior Manager, 2018 Census Field Operations
- Alex Bayley, Senior Manager, 2018 Census Respondent Focus
- Glenn Letts, Project Manager, Channels, Statistics, and Enabling Infrastructure
- Victoria Treliving, Manager, 2018 Census Products and Services
- Kelley Reeve, Senior Manager, Data Futures Partnership
- Heather Jones, Senior Advisor, Strategy, Performance and Privacy (Privacy Officer)
- Tim Henwood, Senior Advisor, Strategy and Development, Data Services
- Anna McDowell, Manager, Integrated Data Infrastructure (IDI)
- Yolandi de Beer, Statistical Analyst, Integrated Data
- Gareth Meech, Senior Manager, Customer Focus (2018 Census)
- Anu Nayar, Partner, National Leader – Cyber, Privacy and Resilience, Deloitte

The following key documents were examined as part of this PIA:

- 2018 Census Design Principles (April 2017)
- OPUS Survey into Public Attitudes to Data Integration (2015)
- Colmar Brunton Use and Trust Survey (June 2016)
- Integrated Data Infrastructure PIA Overarching Document v10 (2017)
- PIA for the Integrated Data Infrastructure (2012)
- Integrated Data Infrastructure extension PIA Fourth Edition (2016)
- Full set of PIAs and other assessment documentation in respect of Census Test
- Full set of existing and contemplated external communications
- Stats NZ privacy guidelines, processes and policies
- Stats NZ De-identification and Confidentiality rules
- 2018 Census Content Determination Framework
- 2018 Census Crisis Communications Approach
- Stats NZ Annual Agency Self-Assessment Report to GCPO (2017)