Document 1

Digital Identity Research

DIA - Proposal

August 2019

Contents

Introduction

1.1 Background

The goal of the Digital Transition Programme (The Programme) is to create the right environment, set the right rules and take advantage of new technologies to give New Zealand citizens secure digital identities that meet their evolving needs and expectations.

The programme is working with citizens, government agencies and the private sector to:

- Make sure citizens have control of what happens to their identity information, including who can use it and how it is used.
- Find out what innovation services the emerging private sector marketplace can offer.

The programme is now exploring options for a new approach to digital identity and research is required to support these options.

1.2 Objectives

More specifically, the primary objectives are to understand and provide guidance about:

- How New Zealanders perceive control over and permission to share their personal information
- How and why that view is formed
- In what situations and scenarios (and why) personal information sharing is more or less acceptable
- Expectations around a Digital Identity Ecosystem including things like common rules and guidelines

Research programme

2.1 How would UMR design and carry out the research?

DIA have already have access to some quantitative research (Unisys 2019 Survey) which investigated consumer support for a number of scenarios around the notion of sharing personal information. Research is now required to better understand why consumers might support some scenarios, but not others, and to identify the factors (conditions) which are conducive and less conducive for sharing personal information.

The best way to understand New Zealander's complex (and sometimes contrary and conflicting!) views, is often to conduct qualitative research; more specifically focus groups.

2.1.1 Discussion

Target Audience

The notion of 'digital inclusion' suggests that research to understand New Zealander's perceptions, views, attitudes and beliefs about control and sharing of personal information, should ideally include all New Zealanders (or as wide a cross section as possible, within the constraints of the research programme.)

There is an argument for focusing the research on people who are more digitally literate and perhaps have a better understanding and a more informed view of the issues and implications of sharing personal information. Conversely, the views and potential misconceptions, concerns and worries of people who are less informed / digitally literate are equally valid, as their limited understanding is likely to highlight very different concerns and perspectives that will be important to understand and mitigate going forward.

2.1.2 Initial start-up workshop

Our usual approach includes a start-up workshop with DIA team members who are closely involved with the topic under investigation. This is an opportunity for DIA to fully brief the UMR team and the UMR team to provide their

insights and debate the research specifications, the topic areas for the discussion guides and input into the development of any prompts, examples and scenarios that can be used.

On this occasion, DIA has already met with senior UMR staff to discuss the proposed research and to informally 'brief' UMR. Also, subsequent material provided to UMR suggests that DIA have a clear idea of their research objectives and what they want covered in the research, so this formal initial stage is perhaps not necessary.

Nevertheless, we do advise meeting again – either face to face or remotely – to discuss and agree the proposed research methodology, the group specifications, the discussion guide and prompts and as the research progresses, to ensure it is meeting DIA requirements.

2.1.3 Eight general public focus groups

Sample specifications

We have outlined some possible specifications for a seven general public focus group research programme that covers a range of New Zealanders but are open to DIA suggestions. We would aim to include a range of ages, gender, ethnicity, working status and life stage across the groups. Also, a mix of people who use ICT more / less often in their daily lives.

We have included cost options for fewer groups and will provide revised sample specification suggestions if one of these options is chosen.

Initially we considered starting this project with a "creativity group". This is a workshop format session, considerably longer than a regular focus group, usually conducted with respondents who have been selected for education and creativity. Essentially, they are recruited to help 'codesign' the discussion guide that will be deployed to the general public in phase two.

While often useful, the downsides are that they typically take longer to organise, are harder to recruit for, and the findings sometimes do not feed directly into the research outputs.

Having reflected on what DIA has already provided, and the background work UMR has done in similar spaces we feel that more value is likely to be gained from heading straight into the focus groups themselves.

Nevertheless, we suggest that the first two groups are recruited to be younger/tertiary educated/more digitally literate – it would be worth testing with them how they feel the general public would perceive the situations we're likely to discuss in these initial groups. Any red flags can then be dealt with prior to groups 2 and 3. This is a fairly common way to proceed.

The below are some suggested specifications for the eight groups:

- 1x general public (tertiary educated, professional, white collar), urban
- 1x general public (tertiary educated, 18-25, tech literate), urban
- 1x Māori, provincial
- 1x general public (blue collar, working), provincial
- 1x Pasifica, urban
- 1x New migrant, urban
- 1x general public, 41-60 years, mix working and non-working, provincial

- 1x general public, 25-40, provincial

i.Development of the discussion guide

DIA have provided a draft discussion guide, which focuses on three broad areas:

- Scenario testing – what people think about scenarios where they have to share their personal information.
- Views of control and permission over personal information online. - Digital identity ecosystem as a concept.

These three broad areas will form the backbone of the discussions. However, to obtain a better understanding of why people respond as they do and to provide context for their answers, we also need to understand a little more about them and what is driving their responses. We have outlined below some examples of questions for the main general public focus groups. These are not intended to be the final discussion prompts, but are illustrative of the kinds of lines of questioning that are likely to be productive.

Background / context setting:

- What comes to mind when you think of "personal information" – what do you take that to mean?
- Share definition
- How often do you share personal information?

Worries/concerns/frustrations about sharing

- What are these?
- Real experiences or potential issues?
- Whose responsibility is it to regulate / allay people's concerns?

General sentiment

- How do you generally feel about sharing personal information?
- What are the main things that influence your views?
- Do you feel you're generally in control of your personal information?
- Is this something you have thought about before? Is this important? Why, why not?
- Whiteboard: What influences your decision to share or not to share?

Portable information

- Have you ever stuck situations where you had to provide information that you expected someone to have already? What about when they already had personal information you didn't expect them to?
- Is portability of your personal information between organisations desirable for you?
- Why/why not? Situationally dependent?
- What advantages / disadvantages might there be?

- Which of these things are most important in terms of making you feel more in control of your personal information? [show prompted list]

Scenario Testing - Drafts

We are now going to look at several scenarios where there may be advantages / disadvantages to sharing your personal information:

- *Doctors sharing your healthcare history with other healthcare providers for a complete view of your health.*
- *A government administrated proof of identity, so you can access commercial services such as bank accounts.*
- *Banks sharing your financial information with other financial service providers to offer you a single point of contact.*

Ask participants to individually rate how strongly they would be to support each scenario and then rank them from the scenario they would be most to least likely to support, then discuss each in turn.

- Reasons for supporting personal information sharing in this instance.
- Reasons for not supporting personal information sharing.
- What gives you confidence?
- What are their main worries and concerns?

- Does who is sharing the information impact your thinking e.g. Healthcare providers, Government (Departments), Banks (Private Financial Providers).
- Who do you trust to share personal information?
- Who don't you trust?
- What reassurances do you need; from whom?
- Should your permission be required; why / not? In what situations / scenarios?
- Would giving your permission make you feel more comfortable; why / not?

Digital Identity Ecosystem

Introduce ecosystem concept:

The government is looking at creating a set of common rules that would allow people, organisations and government agencies in New Zealand to share personal information in a user-consented way, regardless of platform or technology.

It is envisaged that the rules would allow a collection of organisations who provide and use personal information to opt into a trusted, common set of rules that are regulated by government.

The public and private sector could provide products for people to use that would follow the common rules.

- Initial thoughts and impressions.
- What do you like/not like about this idea?
- Does it provide reassurance / allay concerns raised earlier?
- Does it make your more likely to support the above scenarios?
- What would you expect to see in a common set of rules? [prompt if necessary]
- What services, organisations would you like to see that use a common set of rules? [prompt if necessary]
- Should Government and private organisations be subjected to the same rules? Why / not?

ii. Analysis and reporting

We will provide top-line findings after the initial two groups. This will highlight the key findings and provide recommendations for remaining focus groups. All groups will be recorded and transcripts analysed to inform the final analysis and reporting.

A full summary PowerPoint report will be provided that includes verbatim quotes to highlight and provide context to the key findings from the focus groups. See appendix for details on our analysis tools.

2.2 What experience does UMR have carrying out and delivering research of this type?

Several projects which have specific relevance to the requirements of this project are summarised below. In particular, they demonstrate UMR's experience in:

- Qualitative research using workshops and focus groups.
- Research with the general public on issues of public policy and client experience.
- Our willingness to work creatively and innovatively.
- Our commitment to working collaboratively with our clients to achieve the best research outcomes ethically and in ways which benefits and do not harm or upset the participants.

Qualitative research in key policy areas

Much of our public sector research includes areas of change or review around public policy and also New Zealanders service experience of the public sector.

UMR completed qualitative and quantitative research for the OAG in 2012 exploring stakeholder views including the general public on their expectations and views of the OAG to provide input into its strategy development. We are able to use the experience gained from this research and update it for the 2019 research. We note that the focus of this research is different to 2012 but can employ similar methodologies where relevant.

Ministry for Primary Industries: We completed research exploring the changing attitudes towards rural New

Zealand among all New Zealanders. This was a follow-up study to provide further insight into both urban and rural New Zealanders' perceptions of each other over time and all New Zealanders' beliefs and values as they relate to the agricultural, food and forestry sectors. The qualitative stage included 9 focus groups in both provincial, and urban locations in both the North and South Islands. The quantitative survey comprised a telephone survey that included a nationally representative sample of n=750 New Zealanders and a booster sample of an additional sample of 495 rural respondents.

HPA - Parental Supply of Alcohol to Under 18's: The Health Promotion Agency (HPA) is developing strategies to support young people to delay drinking until they are older and to prevent any escalation of drinking if it begins. One of the strategies is to reduce supply of alcohol to under 18s and to enable parents to support their children to remain alcohol-free for as long as possible. Qualitative research was required with parents and caregivers of secondary school age children to understand New Zealand parents' attitudes and approach towards their adolescent's alcohol consumption, with a view to understanding what might work to reduce parental supply to under 18s.

In addition; we have completed research for:

Ministry of Justice: Parents and children's experience of the family court 2014 reforms.

Health Promotion Agency: Stakeholder and general public experience of the Sale and Supply of Alcohol Act 2012 and the development of Local Alcohol Policies.

ACC-Serious Injury: We regularly conduct research among ACC clients who have serious injuries exploring their experience and in relation to specific policy and service improvement initiatives. Most recently the changes to how ACC provides services to clients through a client-centric approach.

Human Rights Commission: Standalone survey on understanding and perceptions of disabled people and qualitative research with the general public and disabled people.

Department of Internal Affairs: Research has included qualitative and quantitative research for the local government commission and stakeholder research for the GCIO.

Inland Revenue: Individual interactions with IR - qualitative case studies.

Customer engagement and consultation workshops

Electricity Networks Association: We have completed a number of stakeholder engagement workshops for ENA as they seek to develop stronger relationships with customers on behalf of their members - lines companies. Lines companies are relatively invisible to customers as the main relationship for customers is through the electricity retailer. Notwithstanding, when there are outages they are at the forefront of the customer experience. Our workshops have helped ENA to explore key issues they face around resilience and reliability of the network and the price-quality trade-offs. All complex issues that are best explored in a workshop session using scenarios and information sharing presentations.

Let's Get Wellington Moving: We worked closely with the LGWM team to develop scenarios of possible transport solutions that the general public could engage with and provide feedback on. The main objective was to workshop these possible transport solutions; refine them and ensure they were easily understood prior to launching them among Wellington community for their feedback.

In addition, we have conducted creativity groups among the general public for New Zealand Police exploring public expectations of policing in the 21st century and a range of other government agencies including the Growth and Innovation Advisory Board and TVNZ.

The research team

We have put together a senior team of qualitative and quantitative researchers who have extensive experience in conducting exploratory and in-depth research on more topics that are not usually top-of mind for New Zealanders.

Alice Kan - Director of Government research

Alice will be the lead researcher for this research and responsible for overall project management and client liaison.

Alice is a specialist social market researcher with a focus on projects designed to achieve awareness, engagement and behavioural change among the public and stakeholders.

She also has a keen interest in public sector research including customer satisfaction and service improvement. Alice has over 15 years in the research industry, as well as prior experience in the public sector, including over six years in the health sector.

Qualifications:

- Research and evaluation of programmes and initiative.
- Workshop and creativity groups design and facilitation.
- Expertise in the development and management of both qualitative and quantitative research projects.
- Experience in research with Māori.
- Research design, sample design, question-line and questionnaire design.
- Reporting and presentation.

Alice has a Bachelor of Science (Biochemistry) and a Diploma in Business Studies. She also regularly upskills by attending the Australasian Evaluation Society Conferences and is a member of the AES.

Relevant experience

- Research with ACC serious injury clients, including young and Māori clients.
- Ministry of Justice research with parents and children who have experienced the Family Justice System.
- Health Promotion Agency - Sale and Supply of Alcohol Act 2012 and the development of local alcohol policies.
- Department of Conservation - qualitative and quantitative research among the general public exploring New Zealanders attitudes, behaviours and perceptions of New Zealand's public land.
- Wellington Water - customer workshops.
- Let's Get Wellington Moving - customer and stakeholder workshops.

Andrea Kan - Executive Director

Andrea will provide qualitative support and back-up on this research and peer review all qualitative and quantitative outputs/ deliverables.

Beginning her career as a quantitative researcher, Andrea has strong statistical and data analysis skills and is one of UMR's in house specialists on quantitative methodology, and questionnaire design. Andrea also remains a "hands-on" qualitative researcher, conducting focus groups and depths interviews on a regular basis and is adept across the full spectrum of qualitative research techniques. She has led and been a key member of research covering the primary sector, biosecurity and food safety.

Qualifications:

- Specialist qualitative researcher.
- Specialist in business research; particularly interviews at the C-Suite level.
- Communications and concept testing for communications campaigns.
- Brand and customer experience.
- Quantitative research specialist; including segmentation analysis and data analysis; an ability to develop appropriate analysis for non-standard projects.

Andrea has a Master's in Business Administration and Bachelor of Science.

Recent relevant experience:

- Multiple positioning and campaign development projects for HPA, including Don't Know, Don't Drink, Oral Health Care, Like Minds, Like Mine, fluoride in drinking water, FAST, Hep C.
- Ministry of Justice research with parents and children who have experienced the Family Justice System.
- Electricity Authority What's my Number campaign development and evaluation and general public research for the Customer Relationship and Engagement research programme.
- Department of Internal Affairs - qualitative and quantitative research understanding customer experience, behaviours and attitudes towards government services.

David Talbot - Chief Executive

David will provide qualitative support and back-up on this research and input into the qualitative outputs/ deliverables.

David is the CEO of UMR and heads the company's political and corporate consultancies. As pollster to the current New Zealand Prime Minister he brings an unparalleled understanding of the New Zealand public mindset to all research projects. His background in communications and campaigning results in highly focussed strategic advice.

Qualifications:

- Specialist qualitative researcher, including focus groups and workshop facilitation.
- Stakeholder and general public customer experience research.
- Communications specialist; specialist expertise in digital communications.
- Brand and customer experience.
- Issue management and strategic development advisor.

David has an LLB and BA (hons) in Philosophy from Otago University.

Recent relevant experience:

- Specialist researcher working with many energy companies including Aurora Energy, Orion Energy, NorthPower and the Electricity Networks Agency. This has required conveying unfamiliar terms and structures to the general public regarding the way power is structured in New Zealand and exploring key concepts from the customer perspective regarding quality, price, resilience, reliability and health and safety.
- Mind and mood of New Zealanders - exploring key issues of the day, including climate change and social media.

Summary of the work programme

We have outlined a draft work programme based on eight focus groups. An updated project plan would be provided once the research specifications are confirmed.

Research components	**Milestones**	**Key deliverables**	**Timing (Date Completed)**
General public - initial two groups	• Finalised discussion guide and prompts • Confirmed specifications for recruitment • Recruitment • Groups conducted	• Recruitment • Groups completed • Top-line summary of key findings • Refinements to discussion guides and prompts for general public focus groups.	23 August 2019
General public focus groups	• Finalised discussion guide and prompts • General public focus groups conducted	• Recruitment • General public focus groups completed	6 September 2019
Analysis and reporting	• Report framework confirmed	• Reporting framework • Draft report • Final report	30 September 2019

Our work programme (prior) indicates specific milestones and dates. We have summarised the key components of the research programme and timeline here.

RESEARCH COMPONENT	DATE
	Week commencing
Initial start-up meeting - completed	Tues 30 July
UMR to provide suggested research method / specifications and timeline	W/C 29 July project
Research method / specifications and timelines agreed – Face to face meeting or remotely	W/C 5th August
UMR drafts discussion guides and prompts for groups	W/C 5 and 12 August
DIA input into discussion guides and approval	W/C 12 August
UMR recruits initial group participants	W/C 12 August
Initial two groups conducted	W/C 19 August
Topline Reporting including implications for future focus groups	W/C 19 August
UMR updates discussion guides and prompts for subsequent focus groups, incorporating findings from the initial groups	W/C 19 August
UMR recruits General Public Focus Groups	W/C 19 August
UMR conducts six general public focus groups (four one week and two the next)	W/C 26 August and 2 September
Reporting framework agreed	(By) week ending 6 September
Transcripts are transcribed, analysis is undertaken, and draft report prepared	W/C 2 and 9 September
Draft report to DIA for comment and approval	W/C 16 September
Final report	30 September
Presentation to DIA (if required)	To be confirmed

Pricing schedule

RESEARCH COMPONENTS	$ EXCL GST
Project management (includes meetings and project updates throughout the programme)	$2,000 research
Initial start-up planning meeting	N/C
Option One	
6 x focus groups (mix of urban and provincial locations; mix of demographics) - Assuming four urban (@$5,500) and two rural (@$6,000) - Hard-to-recruit audiences, if desired (eg rural new migrants) will be estimated separately and may be slightly more expensive or run to groups comprising fewer than 6-8 participants.	$34,000
Option Two	
8 x focus groups (mix of urban and provincial locations; mix of demographics) - Assuming four urban (@$5,500) and four rural (@$6,000) - Hard-to-recruit audiences, if desired (eg rural new migrants) will be estimated separately and may be slightly more expensive or run to groups comprising fewer than 6-8 participants.	$46,000
Reporting	
Analysis and reporting - Toplines – initial two groups - Summary integrated PowerPoint report – all group findings: draft/final	Included
TOTAL PROFESSIONAL FEE	$36,000 - $48,000+GST (Depending on option chosen)
Plus disbursements (estimated):	
6 x Focus groups	$9,000
8 x Focus groups	
ESTIMATED TOTALS	
6 groups (plus estimated disbursements)	$45,000
8 groups (plus estimated disbursements)	$60,000

$12,000

Disbursements are additional and will be passed on at cost. Please note this is an estimate only and once specifications are confirmed an updated cost schedule would be provided. Any direct costs associated with this project will be billed at cost. This includes any staff travel and accommodation, conference room hire and catering and transcription costs. Facilitator incidentals are charged at $100 + GST per day.

Billing would be on the basis of 50% of professional fee on commission and 50% plus costs on completion OR agreed milestones.

If a Word report is required there will be an additional $5,000 + GST.

Company overview

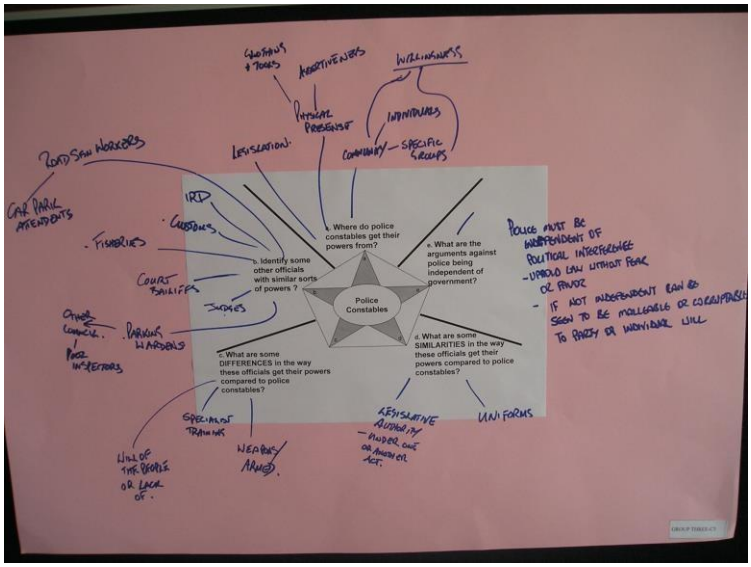
ITEM	DETAIL
Details of owners/ controllers:	UMR is 100% New Zealand owned company.
Size of company:	We have 17 permanent staff and 4 part-time staff in the New Zealand Office. We have offices located in Wellington and Auckland.
Lawyers (name of contact person, phone number, email address and fax number::	Gault Mitchell Richard Martin Ph: 04 472 5074 Fx : 04 471 0835 Email: rnmartin@gaultmitchel.co.nz

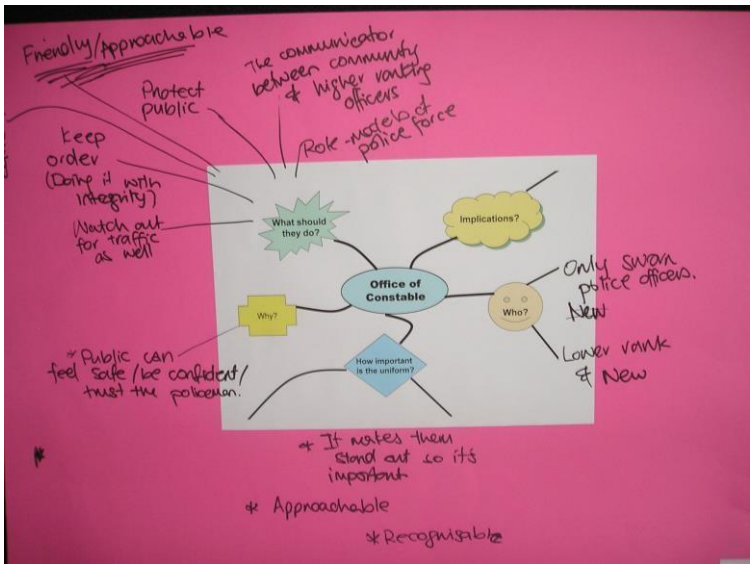
Summary of services provided:	UMR are a full service market research agency with extensive experience. Services provided include: Qualitative research Individual depth interviews, dyads/triads, case studies, focus groups, hall tests, mini-focus groups, qualitative e-panel. All fieldwork and analysis. Quantitative research Telephone, internet, mail (small scale) face to face. All fieldwork data processing and analysis. UMR has a small in-house IQS accredited call centre which is used to conduct small -scale specialist projects and recruitment for our qualitative research. For larger scale telephone surveys we use a specialist research call-centre. Online panels We have a substantial online survey panel. It can be filtered by a wide range of demographics, which means that survey scan be targeted to particular groups of people. Unlike almost all other online panels operating in New Zealand, our panel was initially recruited in telephone surveys. This means that it is not skewed towards younger people and 'technology junkies', which is a common problem with online panels. Desk research Literature searches, internet searches, analysis of existing data/ data collected from other sources.
Industry areas covered:	UMR provides market research services to a range of both private and public sector organisations. Some of our clients include: Major: ACC, ANZ, Auckland Council, Alliance Group Limited, Beef and Lamb, Central Economic Development Agency (CEDA), Chorus, Department of Internal Affairs, Fonterra, Electricity Authority, Health Promotion Agency, IRD, NZ Customs, NZTA, Red Meat Profit Partnership, SkyCity, Spark and Vero. Minor: Auckland Council, Auckland Transport, DOC, Education Payroll, ESR, Insurance Council, LINZ, Massey University, Ministry of Justice, RBNZ, Te Tumu Paeroa, West Auckland Trust, Westpac.
Professional accreditations and quality assurance:	ISO 20252 accreditation UMR was one of the initial groups of market research companies accredited with the Market Research Industry's ISO 20252. All research and data collection activities carried out by UMR are done so to the high standard required by the ISO standard. UMR researchers are also members of the professional bodies such as Market Research Association of New Zealand. Accreditation provides clients with an assurance that quality fieldwork standards are being met, including training, conduct, supervision and quality monitoring. All research staff are members of the Research Association of New Zealand.

Appendix A: General public workshop examples

Our workshops are interactive and activity based and designed to involve participants as partners in the research process.

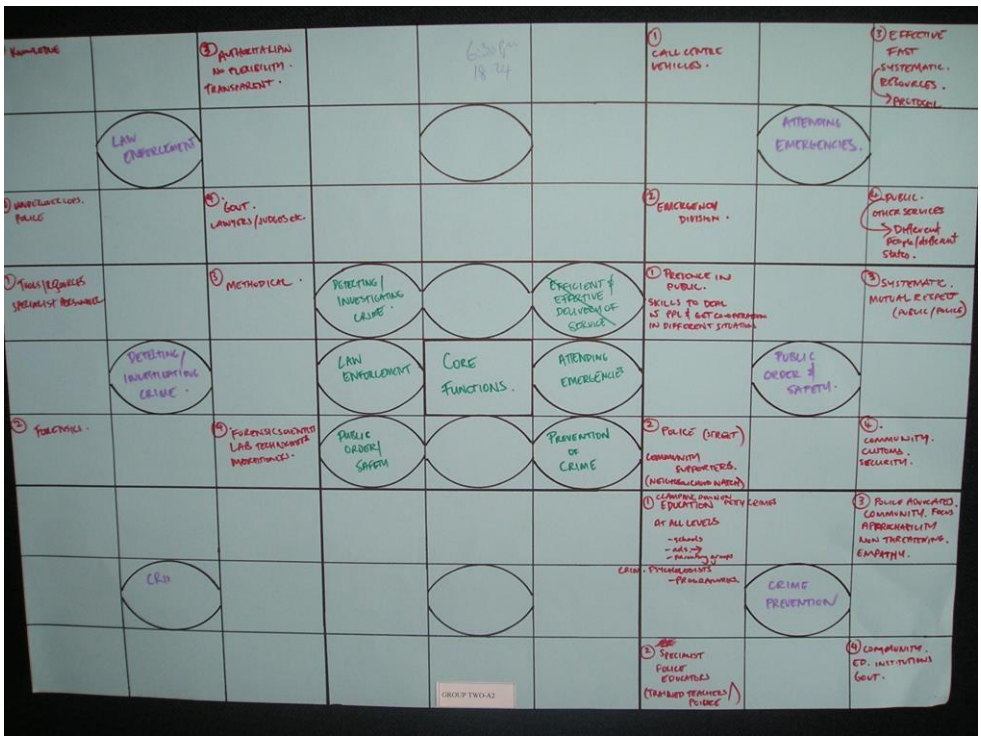
Mind mapping: We use these to help generate discussion and also to support participants to come up with their own reactions and responses - there is the ability to adjust and refine the mind maps as well. The themes from the mind maps generated are collated and identified for further exploration in the focus groups.





Storyboard and card sort example: Participants were asked to explore New Zealand's future using an economic lens. Participants are encouraged to develop the future economic story.

Lotus Blossom activity: This activity was designed to help participants identify the core components and then further develop each of the identified components.



Scenario testing: A number of possible scenarios were presented and participants were asked to 'try' on another hat and look at the scenario from that perspective e.g. from a user of public transport. How believable was this? What would work well? What doesn't work well?

Appendix B: Quality processes

ISO20252

UMR was founded in 1987 and is a full-service market research and evaluation company. We have ISO20252 accreditation, the international industry standard for organisations and professionals conducting market, opinion, and social research.

All research and data collection activities carried out by UMR are done so to the high standard required by the ISO standard. The ISO process requires that quality systems are in place for the collection of data and information and that we are audited regularly.

Our lead researchers work closely with the recruitment team to ensure that only respondents who meet our research specifications are recruited to our qualitative discussion groups. As part of our quality assurance for this project our lead researchers will fully brief our recruitment team face-toface on the research programme and intent. This enables them to more actively participate in the recruitment process.

UMR surveys are most often collected using either telephone or internet methodologies. In either case, industry standard CATI or CAWI data collection programs are engaged to ensure standardised responses and outputs are generated.

the survey instrument; this includes checks on both the wording of the questions and responses as well as the detailed routing of the survey.

In accordance to the ISO 20252 standard, UMR follow a comprehensive procedure for checking and validating any survey script before it goes into the field. This enables our researchers to ensure that the final version of the questionnaire, as signed off by the client, has been correctly programmed.

Ethical practice

UMR staff adhere to the Research Association NZ Code of Practice. The Code has key principles which govern the ethical and professional approach of market researchers. UMR also follows the Guidelines for Ethical Conduct of Evaluations (Australian Evaluation Society Inc). We have conducted a number of research projects that have required ethics applications and are familiar with providing evidence of confidentiality to respondents, information about the research, opportunities to opt out and ensuring that respondents are taking part based on informed consent.

Secure data storage

In line with our accreditation with ISO 20252, our security measures follow industry-standard protocols in all of the above. We operate a firewall and have secure access logins for all staff computers and premises. We promote the use of a secure file transfer service for all confidential files.

Windows server back-ups are written encrypted to an external drive, daily (incremental), weekly (full backup), monthly (full backup). A weekly back-up is sent to Crown Records for secure offsite storage.

Confidentiality agreements

All UMR staff are required to sign a confidentiality agreement at the start of employment with UMR. This requires staff to keep confidential any information acquired in their duties for UMR.

As a company we have also signed confidentiality agreements with some clients (especially when provided with confidential databases of respondents).

Confidential information and documents

All offices at UMR are kept locked when staff are not present. Confidential information and documents are kept in locked filing cabinets. On completion of a project any confidential documents are destroyed by Document Destruction in Wellington and Recall Total Information Management in Auckland or if requested, returned to the client.

Privacy policy

UMR's privacy policy has been written in accordance with the Privacy Act of 1993 and is in line with the requirements of ISO 20252 and the Research Association NZ and ESOMAR code of conduct.

UMR uses the information collected from research participants for research purposes only. We may ask a respondent for their name and contact details so that we can contact them about the research, however, this information will not be passed to a client without the individuals expressed consent.

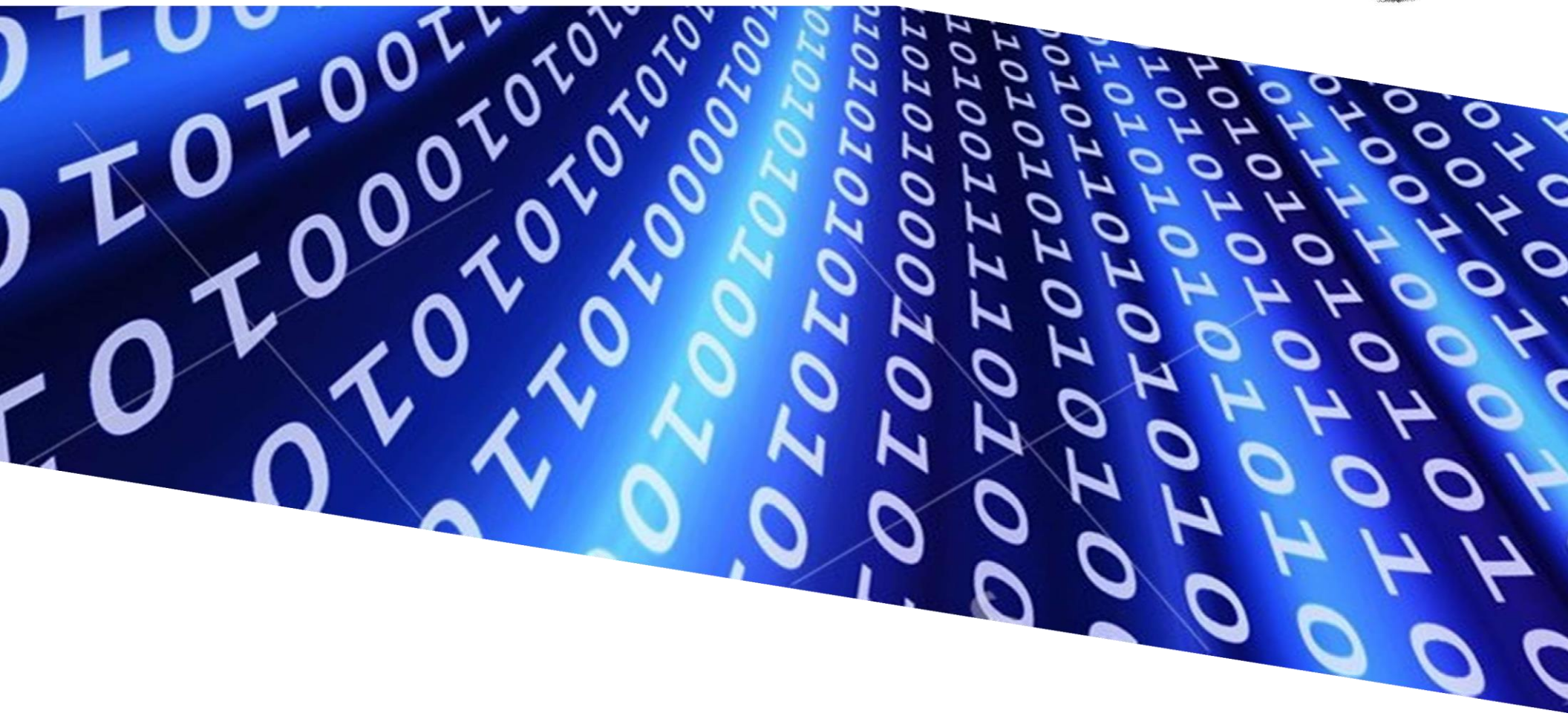
Respondents are made aware, before participation, of relevant information that may affect their decision whether to participate, including the general subject matter, the general purpose of the data collection and the approximate amount of time required to provide responses (unless this is self-evident from the questionnaire).

Data (either qualitative or quantitative) is collated and provided to the client without any identifying responses. Respondents have the right to request access to, and/or correction or deletion of, any information held about themselves by UMR.

Te Tari Taiwhenua
Internal Affairs

Digital Identity Research

UMR



A qualitative study

Te Tari Taiwhenua
Internal Affairs

UMR

Key findings

Personal information

- For many, there was an impression that people had lost control of their personal information as sharing this was necessary to participate fully in modern life. This perceived loss of control colours views on the specific scenarios that were tested and how they protected their personal information, some employing deliberate measures such as avoiding contact and providing inaccurate data.
- All understood the term ‘personal information’ with associations in line with the Privacy Commission definition.
- Most acknowledged the rise in digital service delivery and marketing which had resulted in the monetisation of information.
- Key concerns in relation to sharing personal information revolved around security, misuse of information, and possible surveillance which was seen to breach their privacy.
- Situations where people had felt uncomfortable providing information but had felt obliged to, mostly highlighted instances where there was a perceived imbalance of power such as when seeking financial assistance, in the workplace, when looking to access needed services, and when dealing with government services.
- Most were comfortable with the concept of portable information when it related to sharing information between government agencies, and within the health sector. There were seen to be clear personal benefits to both these scenarios, although they would still want some form of consent process in place. Sharing in the commercial context was not particularly popular, with most believing this would mostly be to the benefit of the commercial enterprise rather than the consumer.

Key findings (cont.)

The scenarios

- The scenario that received the most support was sharing information across the health sector as they could see that this could result in better personal health outcomes. While most could see benefits from government agencies sharing information, the specific scenario of having a government proof of identity was less accepted. Among a raft of concerns, some key issues were that other forms of ID were seen as adequate and some were concerned that it may lead to more intrusive surveillance by the government.
- There was little interest in the scenario where banks could share information with other financial service providers as it was seen to mainly benefit the commercial enterprises and lead to excessive marketing activity.
- In all cases, there would still need to be some sort of consent process in place. On prompting, most preferred a consent process that provided a high level of customisation. This was seen to cater to different types of information and organisations. A simple opt-in process was seen as adequate for basic information, while a default setting would be accepted in the health space so long as the terms and limits were outlined.
- A plethora of reassurances would be required to get any scenario across the line. Applying to all scenarios, participants would like an independent agency that would monitor and enforce rules and for the originator of the data to be responsible for adhering to the rules. For each scenario, specific reassurances were also required which related to how the data could be used in that context.
- On a prompted basis, to feel in control of their information – the top measures for the healthcare and government scenarios were to have limits on the kind of personal information shared and to have government rules on how information might be used/ shared. For the banking scenario, the top measure was to require an organisation to always seek permission from the consumer. This reflected the perception that commercial organisations may flout government rules.
- Security of information covered a range of issues – measures to prevent hacking, oversight that only appropriate people were accessing information/ and that it was being used for the stated purpose, having processes to limit human error, and having a consent process to release information.

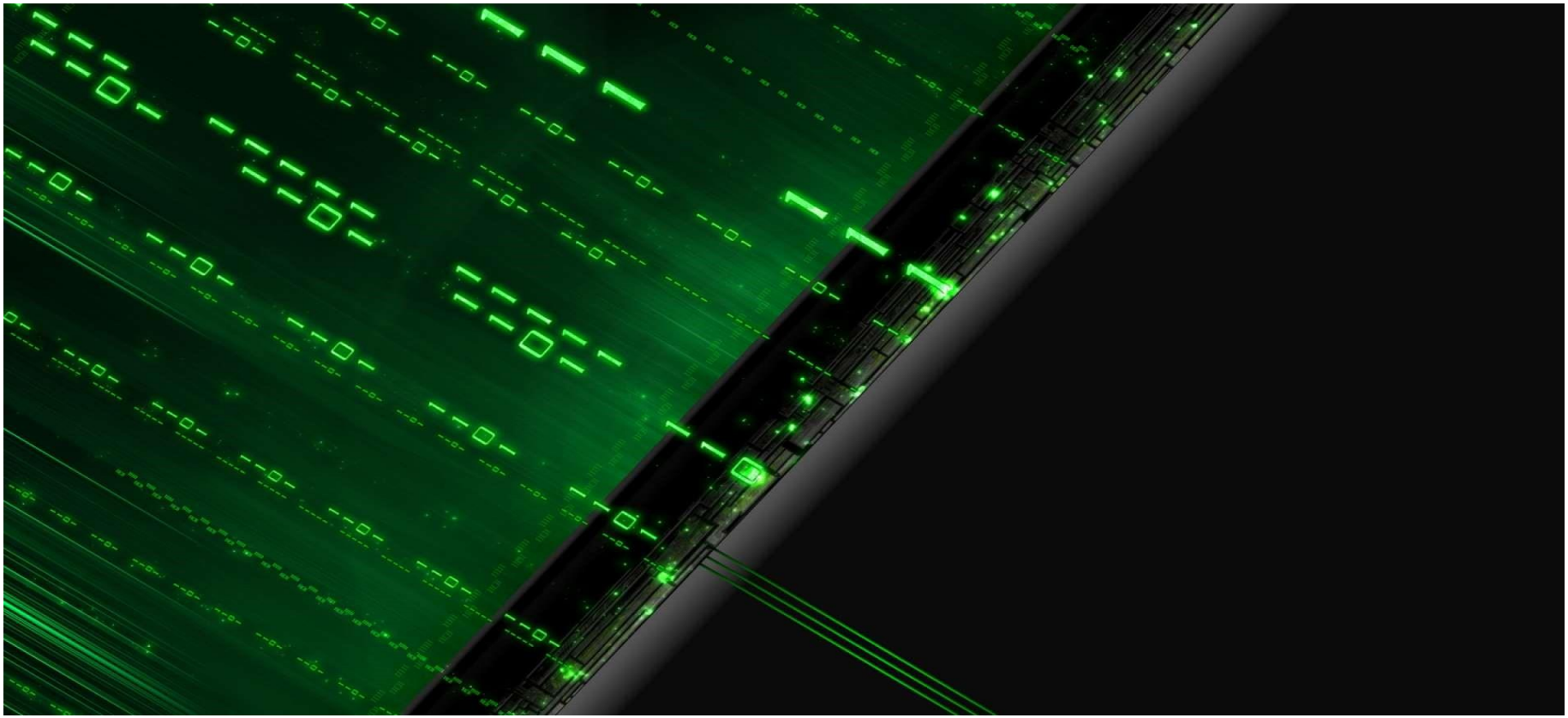
Key findings (cont.)

The ecosystem concept

- There was little support for the ecosystem concept with most unable to see many personal benefits. Negatives were much more emotively outlined than the positives. The key issues of concern were the perceived difficulty to develop and make such a system work, discomfort with commercial entities accessing information held by government, maintaining security of the information, and its potential to erode privacy.
- Concerns would be difficult to overcome as the concept was seen to further reduce the perceived level of control people had over their personal information. To increase support, significant personal benefits would need to be clearly articulated and extensive reassurances outlined.
- People would be open to an ecosystem limited to government agencies and the health sector – although there would need to be extensive consultation with Māori as they did not view the government as particularly trustworthy, in contrast with others, that generally felt the government worked in the best interests of New Zealanders.
- Most felt that the ecosystem would be paid with taxpayer funds. This was another reason not to proceed as many could see more important areas they would like to see taxpayer funds spent on.
- A user pay system where consumers pay was not endorsed as it was seen to penalise low-income households. There was a general feeling that organisations that used the information should pay the costs.

Te Tari Taiwhenua
Internal Affairs

Objectives and approach



UMR

Background and objectives

- The goal of the Digital Transition Programme (The Programme) is to create the right environment, set the right rules and take advantage of new technologies to give New Zealand citizens secure digital identifies that meet their evolving needs and expectations. The Programme is working with citizens, government agencies and the private sector to:
- Make sure citizens have control of what happens to their identity information, including who can use it and how it is used.
- Find out what innovation services the emerging private sector marketplace can offer.
- The Programme is now exploring options for a new approach to digital identity and research was commissioned to understand the views of New Zealanders on these issues.
- The primary objectives of the research were to understand and provide guidance going forward about:
- How New Zealanders' perceive control over and permission to share their personal information.
- How and why that view is formed?
- In what situations / scenarios (and why) personal information sharing is more / less acceptable.
- Expectations of a Digital Identity Ecosystem (Common Rules / Guidelines).

Approach

- The research comprised of eight focus groups conducted between 26th August and 3rd September 2019. The groups were conducted with the following audiences:

Auckland – 26th August, Monday

- 1x general public (tertiary educated, professional, white collar), urban

- 1x general public (tertiary educated, 18-25, tech literate), urban

Auckland – 28th August, Wednesday

- 1x Pasifica, urban
- 1x New migrant, urban

Dunedin – 2nd Sept, Monday

- 1x general public, 41-60 years, mix working and non-working, South Island
- 1x general public, 25-40, South Island

Hawkes Bay – 3rd Sept, Tuesday

- 1x Māori, provincial
- 1x general public (blue collar, working), provincial.

Te Tari Taiwhenua
Internal Affairs

Personal information

UMR

Personal information

- Most participants provided definitions for ‘personal information’ in line with the one provided by the Privacy Commission ‘Data that contains values that identify a specific individual’. The most common association with this term was any information that was specific to a person.
- Younger participants were more likely to consider information on social media as ‘personal information’.
- There was seen to be a major change in how personal information was now shared with a rapid increase in information now stored online.
- The rise in online shopping has meant that people were being asked for contact details constantly. Retailers and service providers were also all wanting to communicate digitally and offering incentives for people to sign onto databases.
- Consumers were aware that personal information has a value and that businesses could use this information to market to them.
- There were concerns about the security of databases and scepticism that these were not shared or on sold to other businesses.
- Some were also sensitive to targeted pop-up advertising that was linked to their browsing history which indicated that someone was monitoring their movements on the internet.
- Frustrations were voiced about the level of spam and marketing communication received, multiple passwords to remember, and lack of clarity around how or who is accessing information.

Views of personal information

Verbatim

I don't know if sneaky is the right word. I think if you look for something and you go on Facebook and the same ad pops up and you get a sense that someone is watching you. That is a bit eerie. But is it sneaky – you know they have access to that information. Auckland, general public, male

I feel a lot more service providers are going online so you feel like you have to sign up for more things. My doctors have all their stuff online, so I have to put all my personal information online for them. Also you become more aware, more cookies collecting information about your browsing history. I guess stories about how they can now use that to identify people.
Auckland, general public, 18-25 years, female

Common typologies

- There were some common typologies evident across the groups in relation to their view of personal information.

Te Tari Taiwhenua
Internal Affairs

Distrustful avoiders	•No benefit from sharing information •Tech savvy, aware of worse case scenario •Avoid sharing where possible, provide false information, have secondary email address
Wary participators	•Growing concern about sharing information •Heard about misuse of information/ breaches •Apply simple security measures - privacy settings, junk mail, reputable sites, secondary email address
Accepting participators	•Relatively relaxed about sharing information •Acknowledge increase in requests for sharing information but sign up regardless •Have little to lose, see little interest in their life
Open embracers	•Not concerned about sharing information •Part of modern society – hear of good deals, get tailored offerings •Want NZ to keep up with rest of world •Believe strict rules around privacy will be enforced

UMR

Concerns about sharing information

- Participants with most concern tended to have experienced or heard of some breach or misuse of data. The increasing amount of information gathered and surveillance (both online and physically) that was happening also made some uneasy. Some felt that modern life was moving in the direction outlined in storylines from books, movies and television programmes they have watched which also underpinned concerns.
- There were more from a Māori and Pacific background that appeared to be concerned about sharing information with particular sensitivity around financial data.
- Migrants were more comfortable sharing information, with many believing misuse of data was less of an issue in New Zealand compared to their country of origin.
- Younger participants raised a wider and more diverse range of concerns.
- Key concerns raised included:
- Being targeted by advertising based off their search history
- Databases being shared – then being targeted by salespeople
- Being scammed and information hacked – identity fraud, bank fraud
- No certainty on where information goes, how it is stored, how it is shared, if information is deleted when requested
- Home automation systems like Google Home and Alexa listening into conversations, tracking search history
- Social media information and photos used inappropriately/ impacting negatively on career
- Surveillance and profiling of citizens by government in other countries (often raised by migrants)
- Signing up to an app on a phone and mistakenly approving access by outside parties to contacts and settings.

Concerns about sharing personal information

Te Tari Taiwhenua
Internal Affairs

Verbatim

I don't like how they want so much I read a lot of sci-fi, so I know where it is all going. I am generally information. And also like everyone is saying an optimist, but it can be dangerous obviously. Information now you can't rely 100% that the information you can be used and we can't even think of ways that it can be used in are giving out is going to be safe. You might 10 – 15 years. So that sort of thing worries me. The amount of find out later that someone has used a information that Facebook and Twitter and even to a point of photo of you or something. Pokemon Go where they are registering where you are walking,

Auckland, Pacifica, male

and they know exactly where you are driving and spending your time. So that type of thing worries me.

Dunedin, general public, under 40 years, male

You get it with the Police all the time too.

My brother had to prove that he wasn't in a certain place, I think it was Wellington, someone used his name and date of birth

and he had to prove he wasn't there. Auckland, Pacifica, male

Everything now is online. And you don't know if you have got a trace following you or anything else. Even insurance, now you have to go online.

UMR

Napier, Māori, female

Control of personal information

- Most participants felt that they had lost control of their personal information. This was mainly due to:
- Feeling they were forced to share information as its part of modern life
- Signing up to too many databases before realising the potential consequences
- The ease of googling and find information about anyone
- Autofill functions on websites
- Being hacked in the past
- No certainty on level of tracking when on the internet.

- Some employed measures that made them feel more in control of their information. More participants from a Māori and Pacific background appeared to be more likely to avoid sharing or provide inaccurate information.
- Measures employed to control the sharing of personal information were:
- Blocking content
- Unsubscribing from websites
- Not opening suspicious emails
- Not signing up or giving information to suspicious websites or with companies they had not heard about
- Reading the T&Cs carefully
- Providing false information such as date of birth
- Having a secondary email address used to sign up for some sites
- Keeping off social media or setting strict privacy settings
- Having spam filters.

NEW ZEALAND INSIGHTS

Losing control of personal information

Verbatim

It is a Catch 22. Living the modern life you kind of have to accept that your information is going risk I guess and if you don't you lose out on some of those aspects of modern technology. general public, male

The second day after I arrived in Auckland many of my friends told me are you alright and my QQ account was hacked and I figured out because I connected to the Auckland WiFi my Chinese email account with my QQ account, three different accounts of mine were hacked and it was sending spam to all my friends. Auckland, new migrant, male

I have probably lost control of it because I have signed up to so many things and I enter heaps of competitions and that kind of thing, so you are giving your information. Auckland, general public, female

Situations where felt uncomfortable

- Only a few situations were recounted where people had felt uncomfortable providing information but had felt compelled to provide it. The situations could be grouped into broad categories.
- Financial – people were very sensitive to the need to provide personal financial information even if it was to access services.
- Loan applications where they had to provide what they felt was overly intrusive or long-term information on spending and earnings

- Tenancy agreement where they had to provide payslips over several months.
- Workplace – in the workplace they felt unable to refuse what was seen as an intrusive level of monitoring of internet usage and personal content.
- Viewing of personal content over WiFi and using it against people.
- Services – when signing up for services or resolving service issues, some had reluctantly signed up or provided information.
- E-scooters sign up which required a drivers licence, passport, bank account
- Access to apps
- Confirming booking
- Seeking a refund from an airline.
- Government – providing information to keep benefit payments, filling out Statistics New Zealand surveys which were a legal requirement but included intrusive questions around business practices and financial details.
- Statistics New Zealand survey
- Purchasing a house when receiving government support.

Uncomfortable sharing information

It happens when you download an app and it asks for all these random things. I am not happy, but I need to because I need to use the application and it needs access to my camera, my microphone, my contacts. [Why do you need that app?] It is a cool app.

Auckland, new migrant, male

Verbatim

I have just bought a house and once again the information I had to give to the government departments about where I got the money from and all sorts of other

bits and pieces. I wasn't happy doing that. Dunedin, general public, 41-60 years, female

Previously, to sign tenancy agreements for houses… I have had to give them actual pay slips to prove that I earn money. And that is something that I am not comfortable with, but you don't want to be homeless at the same time. Auckland, general public, female

I sort of feel that way if you have to use a company's WiFi and you don't have the option. [Because you have to use the WiFi?] Yes. There was a bit run where someone would post a photo of themselves drinking or whatever and then they would get drug tested or alcohol tested. Auckland, general public, male

Te Tari Taiwhenua
Internal Affairs

Provision of information when expected to have or vice versa

- Most instances where people expected information to be stored but it was not – related to interactions with government. It was clear that most believed or expected many government agencies to share information. Examples included:
- Lack of free-flowing information between DHBs, GPs, specialists
- IRD where they expected forms to be auto-filled from previous contact or being asked for details when they had contacted them
- Immigration New Zealand which asked for the same information multiple times
- StudyLink having no link with IRD.
- Only a few commercial examples were raised:
- Payment details not being saved from past transactions
- Bank requiring tax details
- Power company requiring contact details
- Telecommunications company requiring contact details for an ongoing service issue.

- There were fewer situations where an organisation had had information when they had not expected it. This tended to be the reverse with commercial situations dominating and included:
- Pre-filled fields on websites when they had not asked for details to be saved in the past • Lay-by details saved with a store they had not dealt with before
- A bank that had recognised them from their phone number.
- In the government sector situations recounted were where IRD had calculated a tax rebate without any contact, and contact details being known when ringing the police.

Situations when had more information/ less information than expected

Verbatim

So if someone is allergic to some kind of medicine and they have never been to hospital before they have no idea. I thought they would know everything. Auckland, general public, male

[Examples when they had more information on you than you expected.] If you have logged into that website before and you exit your Firebox or whatever and then you go on it again. And you go to enter your details and sometimes they are pre-filled in.

Generally when you apply for StudyLink and it requires your IRD I assume they are connected, and it makes sense that they would be. If they are not you are bit like well, what is happening with my money. Auckland, general public, 18-25 years, female

Auckland, general public, 18-25 years, female Signed up for layby and it said log in and... it asked for my number or email and I put in my number… and it came up with my Eftpos card.

[Chance you had signed up before?] No, I signed up with a totally separate company, Afterpay is from

overseas and Layby is a New Zealand company.

Auckland, Pacifica, female

Portable information

- The strongest case for portable information was in the government and health space. However, even with government a number would only like information shared if consent was given. Trust in the organisation receiving and holding the information was key, which was a strong reason people were more comfortable with the government sharing information. People could also be convinced if there were real perceived benefits and the type of information being shared was limited such as could be found in the White Pages.

Case for portable information

• The concerns with portable information were:

were:

used against you with specific examples relating to

government agencies using information to cut benefits or pension
StudyLink

collected

Case against portable information

- In relation to government services and healthcare, the positives

• View as a slippery slope where more and more information would be

- Trust the government to keep information safe shared
- Can identify criminal behaviour/ abuse• Information could be

- Logical for some services to be linked such as IRD and

• That information could be misinterpreted without having the context of

- Create efficiencies and save money

where and how it was

Difficulty changing inaccurate information if you don't know the origin

personal • Some general positives were:

identity

can't be trusted – no guarantee information is

over who sharing with, open to cold calling

- Lead to better health outcomes. •
- Dislike the thought of sharing financial information which is too
- Security issues - past security breaches, potential to be hacked,
- Will make interactions faster and easier theft
- Won't need to repeat information • Commercial enterprises
- Will get targeted relevant information, offers secure, no control
- Less paperwork. • Prefer to be in control of information

Views of portable information

It costs less to have one person collect the information.
Auckland, general public, 18-25 years, male

Verbatim

But I think the individuals that are in control of that information have to be scrutinised completely. Individuals who are able to access the information are they able to be trusted?
Napier, Māori, male

I think it is a trade off, what do you receive in return for sharing your information. Auckland, general public, 18-25 years, male

Maybe better use of their resources. They could condense their resources like they did with ACC and started shutting down all the offices. Dunedin, general public, 41-60 years, male

I guess if you take a step then where is the next step. I don't have an issue with this, but does it open a gap for something else. Dunedin, general public, 41-60 years, male

Te Tari Taiwhenua Internal Affairs

Key insights

- There was little ambiguity in regard to what people perceive as 'personal information' with associations in line with the Privacy Commission definition.
- Most acknowledged the rapid increase in sharing of personal information with the rise in digital service delivery. All realised that their personal information had value to commercial enterprises.
- With the rise in digital interactions, concerns were evident. The key issues were around security, misuse of information, and possible surveillance which was seen to breach their privacy. Sinister themes from popular culture were reinforcing potential concerns around surveillance.
- A majority felt they had lost control of their personal information as they believed sharing information was now necessary to participate fully in modern life, with many also acknowledging they had signed up to numerous databases and services which required sharing personal information. This loss of control helps inform views on the specific scenarios that were tested.
- Some did employ measures to control the information they shared – at the extreme end avoiding contact and providing inaccurate data.
- A number of situations were recounted where people had felt uncomfortable providing information but had felt obliged to. Most were situations where there was an imbalance of power – seeking financial assistance, in the workplace, to access needed services, and when dealing with government services.

UMR

- People were much more likely to be able to outline situations where they had had to provide information they expected an organisation to already have, compared with being surprised when an organisation had more information than they expected.
- Most were comfortable with concept of portable information when it related to sharing information between government agencies, and within the health sector. There were seen to be clear personal benefits to both these scenarios, although they would still want some form of consent process in place. Sharing in the commercial context was not particularly popular, with most believing this would mostly be to the benefit of the commercial enterprise rather than the consumer.

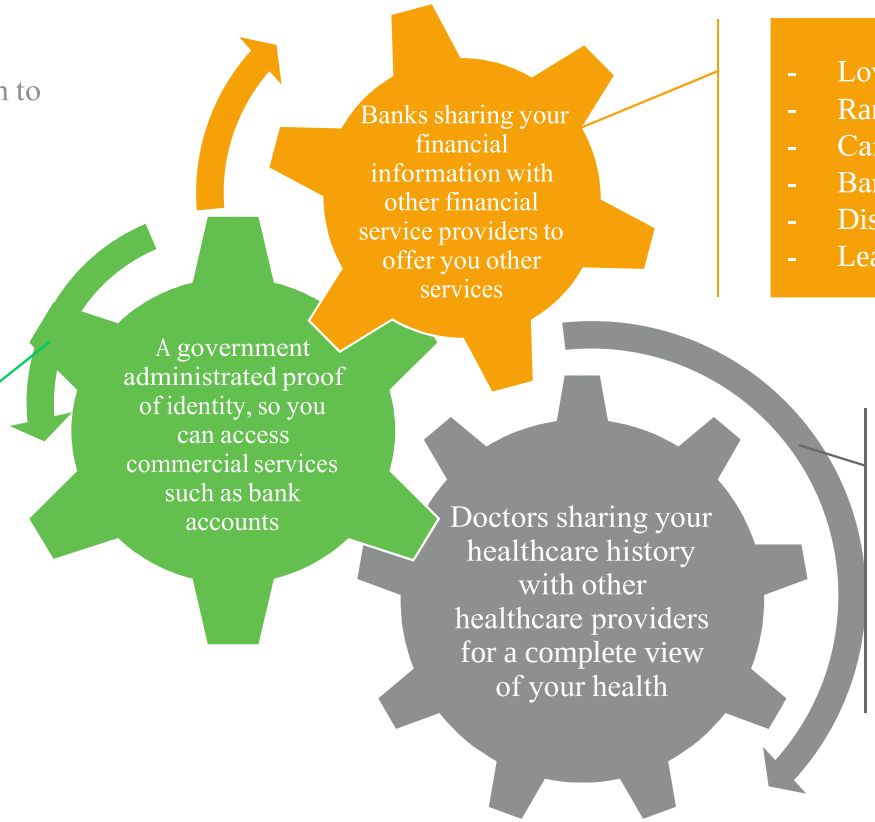
Te Tari Taiwhenua
Internal Affairs

Scenario testing

UMR

Preferred scenario

- The healthcare scenario received the most support, mainly due to it leading to better health outcomes.
- The government proof of identity did have some support, as a majority did trust the government to hold information, but it was seen to have minimal benefits.
- The bank scenario had weak support, as the bank was seen to benefit the most from the arrangement.



- Low support – 2.3 out of 10
- Ranked last by 50/ 59
- Cannot see personal benefit
- Banks please shareholders not consumers
- Distrust banks
- Lead to more advertising, sales calls

- Medium support – 5.7 out of 10
- Lower support among Māori and higher across migrants
- Ranked second 46/ 59
- Benefits less clear but potential for some
- Trust government/ accountable
- Try to do best for New Zealanders

- High support – 8.6 out of 10
- Ranked first by 52/59
- Seen as essential by many
- Can see a clear personal benefit – with information sharing resulting in better care

Healthcare scenario

Doctors sharing your healthcare history with other healthcare providers for a complete view of your health

•Participants were most comfortable with this scenario. They could see a clear benefit to sharing information in the health context. However, many still wanted to have to give consent for information to be shared. They wanted control over the release of sensitive information, the type of healthcare providers it was accessible to, and what the information would be used for.

Positives

- Result in better care
- Provide information if unconscious or incapacitated
- Cannot see any disadvantage
- Don't need to repeat information to every healthcare provider
- Record of information they may have forgotten
- Trust healthcare providers especially GP

- Concerned about what type of healthcare provider has access – needs to be in relevant to primary care
- Don't want sensitive information released that is not relevant to current care, particularly, sexual history, mental health
- Prefer to outline information personally so can explain history and context
- Information maybe misinterpreted

Healthcare scenario

Verl

- Healthcare providers can be more efficient, make their job easier
- Help with transient, moving population.

Negatives

- May be used against you such as insurance companies declining cover
- Open to liability issues
- Staff unrelated to healthcare may look at information.

I feel that it is essential. If you have got a health condition having to go from organisation to organisation and health organisation and have to explain yourself all over again. If they have got the whole thing there and they have shared that information across those health providers that you are involved with it makes the process so much easier. Napier, rural, Māori, female

I feel like the potential for that to be really important ~~to save your life would be quite high and the potential~~ for harm aside from maybe some embarrassment if you have got an embarrassing health condition is fairly low.
Dunedin, general public, under 40 years, female

I am unclear who healthcare providers could be, could it be a minor healthcare provider. Depending on how strict that is. [What do you mean by a minor healthcare provider?] Say you had a mole or something and you go to a dermatologist or something – is that a healthcare provider. You don't want them to know about all your counselling history.
Auckland, general public, 18-25 years, female

Healthcare scenario – control of information

- For the healthcare scenario, the measures that would make them feel most in control of information were having limits on the kind of information to be shared, having government rules, and requiring organisations' to always seek permission.

Limits on the kinds of personal information that can be shared	•Means can control sharing of sensitive information •Ensures only information that is relevant to particular health providers is shared
Government rules that specify now it might be used/shared	•Blanket rules can cover all issues •Ensures national consistency •Implies government will enforce the rules
The requirement for organisations to always seek your permission	•Provides total control •Lower rating compared to other scenarios as may not be in a condition to give permission
Your relationship with the sharer	•Indicates the type of information that will be shared •Depends on level of trust in sharer
Your relationship with the sharee	•Ability to check if sharing the information will benefit them •Depends on level of trust in sharee
Limits on the time personal info is shared for	•Information may not be relevant to future care •Once health issues resolved may not be relevant

Government proof of identity

A government administrated proof of identity, so you can access commercial services such as bank accounts

•Participants were polarised on this scenario – while some were reasonably relaxed, others were concerned that this would be the first step in the government extending its control and monitoring of citizens. Even those relaxed with the concept, questioned whether the benefits warranted the cost to set up and maintain such a system.

Positives

- More secure, less open to identity theft, harder to fake
- Only need one ID, convenient
- Easier to replace if lost or stolen
- Less paperwork when applying for services
- Less need to repeat information
- Works well in other countries (migrants)
- It's the future, way the world is going
- Provide identification to get benefit if homeless.

Negatives

- Concerns about government control, know too much, lose individual identity – just the beginning and may lead to facial recognition etc. Related to this, it depends on who is in government
- Cannot see the benefit – already have plenty forms of ID, drivers license, passport, 18+ card
- Concerns about security – having so much linked to one ID, more attractive to hackers
- Concern about being linked to commercial services like bank accounts. Financial information is viewed as particularly personal
- Opens up data sharing with commercial organisations – concerns about what information will be used for and who it will be shared with
- Will require significant costs to set up and keep up to date.

Government proof of identity scenario

Government administered proof of identity. That is really important in terms of we can rely on one form of identity which is valid. Given that you can make fakes so easily now and it happens to be that you use that proof of identity to access commercial services.
Auckland, general public, 18-25 years, female

When you use the bank, they want your bank card and your drivers licence, so it would just be like a drivers licence but not a drivers licence – that is how I saw it. I pretty much already have a drivers licence. It seems like we are already dong that anyway.
Dunedin, general public, 41-60 years, male

Verbatim

It just streamlines things a lot faster, I think. To run around three different places around town just to get one document done for example.
Dunedin, general public, under 40 years, male

I think they are going down a rabbit hole personally. I remember getting my licence in 4th form at high school and it was a paper one with no photo, just paper and that sufficed. Now we are getting more technological, more advanced yet that is still not enough. No matter what we have got today, photo ID, a RealMe account it is not enough you need more. I think it is going to end up that they think they are righteous enough to make decisions for us to play God. Napier, Māori, male

Government proof of identity scenario – control of information

Te Tari Taiwhenua
Internal Affairs

- For the government proof of identity scenario, the measures that would make people feel most in control were similar the healthcare scenario – having limits on the kind of information to be shared, having government rules, and requiring organisations' to always seek permission. Although the reasons for these choices were slightly different.

Limits on the kinds of personal information that can be shared	•Requirement for limit as government holds a lot of information on people •As sharing with commercial organisations would want to be specific about the information that can be shared
Government rules that specify now it might be used/shared	•Provides clarity on rules that would apply •Trust government to set rules •Assume will be governed by legislation and will be monitored and enforced
The requirement for organisations to always seek your permission	•Provides total control •Need this control as government holds sensitive information and going to commercial organisations
Limits on the time personal info is shared for	•Financial information dates fast •No need to hold irrelevant information
Your relationship with the sharee	•Depends on level of trust in sharee
Your relationship with the sharer	•Depends on level of trust in sharer

UMR

Banks sharing financial information

Banks sharing your financial information with other financial service providers to offer you other services

•Participants were not comfortable with this scenario. They struggled to think of personal benefits arising from this initiative, mainly as they felt banks were commercial enterprises that would use the information to increase sales and benefit the bank, rather than consumers.

Positives

- Could make it easier to get a loan/ access other financial services
- Identify services they might need
- Trust bank to use information appropriately
- If sharing information with government, may be able to identify support that people are missing out on • Identify abuse if inappropriate spending while on benefit
- Can automatically put on appropriate tax rate.

Negatives

- Will result in more sales calls
- Information held by banks is personal financial information which they don't want to share
- Will benefit the bank – they want to maximise profit, not work in best interests of customers
- Unclear who they will share information with
- No say who runs banks, unlike government
- May make it harder to access credit
- Prefer to provide information directly
- Information could be used inappropriately such as being targeted by loan sharks.

Bank sharing information scenario

Verbatim

May make things easier when you are going for loans or trying to find a second mortgage or whatever.
Napier, rural, Māori, female

It helps you be more compliant. Say you have investment you are not aware of how much money you are actually making rather than waiting for the IRD to come knocking and smack you on the hand.
Auckland, general public, 18-25 years, female)

So to me that is trying to upsell me for health insurance or life insurance, home and contents and all of that... Like you should have this type of insurance because it is way better than what you have currently got. 99 times out of 100 they are just trying to cash in and sell me something that is not actually going to benefit me.
Napier, rural, Māori, male

Bank sharing information scenario – control of information

- For the bank sharing information scenario, the measures that would make them feel most in control were quite different to the other scenarios. Requiring organisations' to always seek permission was the clear frontrunner, followed by having limits on the kind of information to be shared, with having government rules a distant third.

The requirement for organisations to always seek your permission	•Provides total control •Can determine whether sharing information will benefit them •Cannot rely on rules as banks often flout them
Limits on the kinds of personal information that can be shared	•Provides them with assurance that particularly personal financial information will not be shared
Government rules that specify now it might be used/shared	•Government needs to enforce and ensure rules are followed
Limits on the time personal info is shared for	•Financial information seen as particularly time sensitive •Do not want indefinite access
Your relationship with the sharee	•Want to know if sharee is commercially driven
Your relationship with the sharer	•Depends on level of trust in sharer

Reassurances

- There were some reassurances to allay concerns that could apply to all the scenarios, which included:
  - Having an independent government agency to monitor and ensure rules were adhered to
- Identifying the originator of information with associated accountability.
- Other specific reassurances are outlined below.

Healthcare scenario

- -Ensure only used in relation to their healthcare
- - Provide a definition of 'healthcare providers' that would have access
- - Provide rationale for having to provide information

Government identity scenario

- - Would require backup if system went down
- - Need to be able to opt-in and opt-out
- - Needs to be policed so information used appropriately

Bank sharing information scenario

- - Only have ability to share very basic information
- - Limiting marketing activity
- - Need to be able to opt-in and opt-out
- - Needs to be policed so information used appropriately

Giving consent

- Participants were most likely to choose the consent process that gave them maximum control of their information. A more detailed consent process was seen to provide the best protection when different types of organisations and different types of information may be shared.
- Some would be comfortable with a less stringent consent process if the information was more basic or being shared with a trusted organisation.
- To provide additional reassurance a few suggested that the owner of information could access the search history so they could see who had been looking at their information. A step further, some wanted to be notified and asked consent when a person wanted access.

Detailed consent

- Gives the owner of information the most control
- Allow for different options for different types of information and different organisations
- Will make people read and go through process of considering each type of information

Opt-in

- May need a default process for important information like health
- Still have reassurance of some control
- Appropriate for simple information
- Like simplicity
- Would like a double opt-in process so that people clearly understand what they are agreeing to

Default

- Seen as most appropriate for healthrelated information so that optimal health outcomes are achieved
- Need clarity and education about what rules are covered by default
- Needs to be enforced with legal consequences

Giving consent

Verbatim

[Default.] For me the way around it would be having the first option where you have a level of agreed information that goes out and it is blanket because that way you avoid the subjectivity of what is important and what is not. It depends on the scenario but putting it into healthcare absolutely I would not trust the general population to figure out what is important in their health and what is not. Auckland, general public, male

Detailed. I like that approach. Sometimes if there is some information you ask them where are they showing this and you don't mind because it is your name and age and it doesn't give much information. Auckland, new migrant, male

Personally, I think it would be in my best interests to go through and tick exactly what you do and don't want. Auckland, general public, female

I don't like the default things because sometimes you can misunderstand what the default is, personally. Dunedin, general public, 41-60 years, female

I think I would still want to have some control when it is something easy that you can personally tick. Dunedin, general public, 41-60 years, female

I think probably Option 2. It is pretty easy to tick on something and say I consent to this being shared or not. Auckland, general public, male

What does ‘secure’ mean?

- Many mentioned that they wanted reassurance that information was kept secure. This covered many aspects including:
- Measures to prevent hacking and continually keep up to date
- Oversight to ensure non-authorised people were not looking at information
- Ensuring there were processes to minimise human error and accidental leaking of information
- Ensuring that information was accessed and used for the purpose it was collected for
  - Inability to release information without permission.

For me it is not being hacked it is not being abused. So you keep it safe. I don’t know who can get access to that information. Auckland, new migrant, male

They can’t just release it. I know that people hack into things but as secure as it can be at this time. Dunedin, general public, 41-60 years, female

Your personal things have not been exposed to other people. For example nowadays in this country people are not much worried if a person is gay but back in our country, they make it an issue.
Auckland, new migrant, male

Sharing ‘date of birth’

- Most were not keen for ‘date of birth’ being shared by a commercial business like a bank – or even a government agency, unless it was being shared with another government agency.
- The main reason for this reticence was that ‘date of birth’ was often used as a way to confirm identity and linked to passwords.
- In regard to a bank sharing such information, they could see no personal benefit or need for this to happen.

> [Bank sharing date of birth.] I don’t think they should be giving any of your information to anyone. I don’t think it is beneficial to me.
> Auckland, general public, female

Key insights

- Sharing information across the health sector was endorsed by participants as they could see that this could result in better personal health outcomes. There would still need to be some sort of consent process in place, particularly in regard to the health providers that would have access to information and the type of information that could be shared.

- While most could see benefits from government agencies sharing information, the specific scenario of having a government proof of identity was less popular. It was seen as unnecessary as there were other forms of ID and some were concerned that a universal ID may leave to more intrusive surveillance of citizens by the government.
- There was little interest in the scenario where banks could share information with other financial service providers. This was seen to predominantly benefit the bank and other providers rather than the consumer, and lead to excessive marketing activity.
- An independent agency that would monitor and enforce rules and having the originator of the data being held accountable would provide some reassurance in regard to all scenarios. There were some specific reassurances in relation to the healthcare scenario around the information only being used in relation to their personal healthcare, having a defined list of providers that could access information, and the provider having to note why they needed access. For the government proof of identity, they wanted stringent security and backup systems, an ability to opt-in and opt-out later, and policing of the use of data.
- Across prompted measures that provided control of their information – the top measures were consistent for the healthcare and government scenarios being the need to have limits on the kind of personal information shared and government rules on how information might be used/ shared. This was different for the banking scenario with the top measure being requiring an organisation to always seek permission. This reflected the perception that commercial organisations were seen to flout government rules.
- Most preferred a consent process that provided a high level of customisation. This was seen to cater to different types of information and organisations. A simple opt-in process was seen as adequate for basic information, while a default setting would be accepted in the health space so long as the terms and limits were outlined.
- Security of information covered a range of issues – measures to prevent hacking, oversight that only appropriate people were accessing information/ and that it was being used for the stated purpose, processes to limit human error, and a consent process to release information.

Te Tari Taiwhenua
Internal Affairs

Ecosystem concept

The government is looking at creating a set of common rules that would allow, organisations and government agencies in New Zealand to share user-consented personal information, regardless of platform or technology so long as they opt into the shared set of rules. These rules would be regulated by government

UMR

Views of ecosystem concept

- There was a lacklustre reaction to the ecosystem concept with negatives being more intensely voiced than positives. The key issues were an inability to visualise major personal benefits from the concept, the difficulty to develop and make such a system work, discomfort with commercial entities accessing information held by government, maintaining security of the information, and potential to erode privacy and liberty.

Positives

- Simplify information storage – one password, one ID
- More efficient, less repetition
- Reassured if have a good set of blanket rules/ security measures
- Keeping up with the rest of the world, way the world is going
- May lead to better delivery of support services, if all agencies are sharing information
- Identify fraud
- Provide Census information

Negatives

- Struggle to see personal benefit
- Will be difficult to develop a common set of rules that will work – as will need to cover diverse organisations, diverse information, diverse platforms
- Dislike commercial organisations being able to access same information as government – will use it for own benefit
- Slippery slope – intrudes on privacy, attack on liberty, veering towards socialism, government spying, loss of control
- Security issues – all organisations won't have same security set up, more attractive to hackers as information held in one place, don't trust government to manage
- Will be too big and costly to set up and manage
- Already have Privacy Act to protect information
- Opt-ins/ opt-outs – reduces validity of data, implied threat to those that opt out that they may miss out on services
- Prefer to focus on improving sharing of information within government agencies

Views of ecosystem concept

From a very simple level it would be on one password. I guess it would be an efficiency thing. The perception is very streamlined and also the perception that these common rules are protected by one security measure not separate things. [So there are a robust set of standards.] With a blanket set of rules I would say

would come a blanket set of security measures. Auckland, general public, male

It seems to me that it is taking control away from people in a way. I would like to be in control of my own life as much as possible. This one seems a bit like if you don't opt in then you would be left behind sometimes. In a way it is almost like forcing you to do it.
Dunedin, general public, 41-60 years, female

People don't want their control being taken care of by someone. Where is the information being stored, who is sitting in front of that massive country computer pushing the buttons. What if he falls asleep, what if someone hacks it. There are so many unknowns. Auckland, Pacifica, female

If it becomes compulsory, then it is going down the mark of the beast type of thing. We are talking about you must have this to survive and if you don't have it you can't survive. I haven't got one of these cards, you can't open a bank account. You can't open a bank account you can't get your benefit, you have no food, no money. Napier, Māori, male

Providing reassurance

- It was clear that many measures would need to be set in place for people to even be open to the concept. On an unprompted basis, reassurances raised by participants were:
- To be regulated and monitored by an independent agency as governments come and go
- Rules around the types of companies that would be included in the ecosystem
- Needs to be enforceable by law
- Preference to limit to New Zealand organisations
- Rules around the type of information shared, justification for sharing information
- Assurances that rules would be monitored and enforced
- Requirement for all parties to have adequate security systems
- Assurances information would not be used for marketing or spam
- Allow optional opt-in and ability to opt-out in the future
- Ability to review information held about them and correct it.
- Prompting about participating organisations being accredited, most did find this reassuring as it implied that an independent agency would be managing the process. People liked the idea that they could look at a list of accredited organisations before opting in. However, most would still want to choose which organisations on the list they would be comfortable accessing their information.
- As we had tested the banking scenario earlier, some did think banks and other financial providers may be included in the organisations accessing the ecosystem. However, for some, the current description implied that it would only apply to government and non-commercial organisations like charities, associations and societies.
- People were generally more comfortable with it being limited to these non-commercial organisations.

Providing reassurance

Verbatim

I don't like the word organisations because that is [You want to know who these government they are regulated by an independent organisations are?] I want a list. I like the authority. Governments come and go. government agencies I just don't like the word organisations because that could be anybody. Auckland, new migrant, male Dunedin, general public, 41-60 years, female

I would think rather than be regulated by very broad.

How plausible are these common rules or are they all just going to be principles which tell people off if they are not following them. What are the consequences if you don't do them. Auckland, general public, 18-25 years, female

How difficult would it be to change information on information?] Yes. And how far does the personal information go is it how many kids you have, do you have a partner, relationships change all the time.
Dunedin, general public, under 40 years, female

there. [You would want to be able to go in and change your

Rules for government and private organisations

- Most could not see how the same rules would apply to government agencies and private organisations. The information held by government was extensive as people often had no choice but to provide this information. Therefore, if private organisations were in a position to access this information, they wanted strict rules in place on what information they could access and which organisations.
- It was acknowledged that private organisations would not necessarily do what was in people's best interests so needed rules to govern information use, while government agencies were generally seen to work for the people.

> [So what is the main difference between the government and a private company?] I would hope the government was trying to do better for me and everyone around me. Whereas the company is trying

to please the shareholders or whatever. Auckland, general public, 18-25 years, female

Funding

- Most felt that it sounded like taxpayer funds would be used to develop and maintain the ecosystem. In general, perceived benefits were not seen to warrant the cost to taxpayers and most would prefer funds to be spent in other areas.
- New Zealand was seen to be a small country that did not need such a system when there were so many other issues to resolve. To change their minds, stronger benefits would need to be outlined to justify the cost.
- If a user pays system was implemented, they felt it might disadvantage those on lower incomes, especially if not being part of the ecosystem meant people would miss out on services.
- User payers was considered more appropriate for the organisations that used the information as they were seen to benefit directly from its use.

But how are they going to regulate every company and organisation within New Zealand. What is

that going to do to taxpayers' money, they are going to have to set up this whole department just to look after this one scheme and we all pay for it so that all these

sectors can share information that they don't need. Auckland, general public, female

Then the other end if it was a user pays system, I don't really see it being effective because it would either die out or you would struggle to get a lot of people on board. Auckland, Pacifica, female

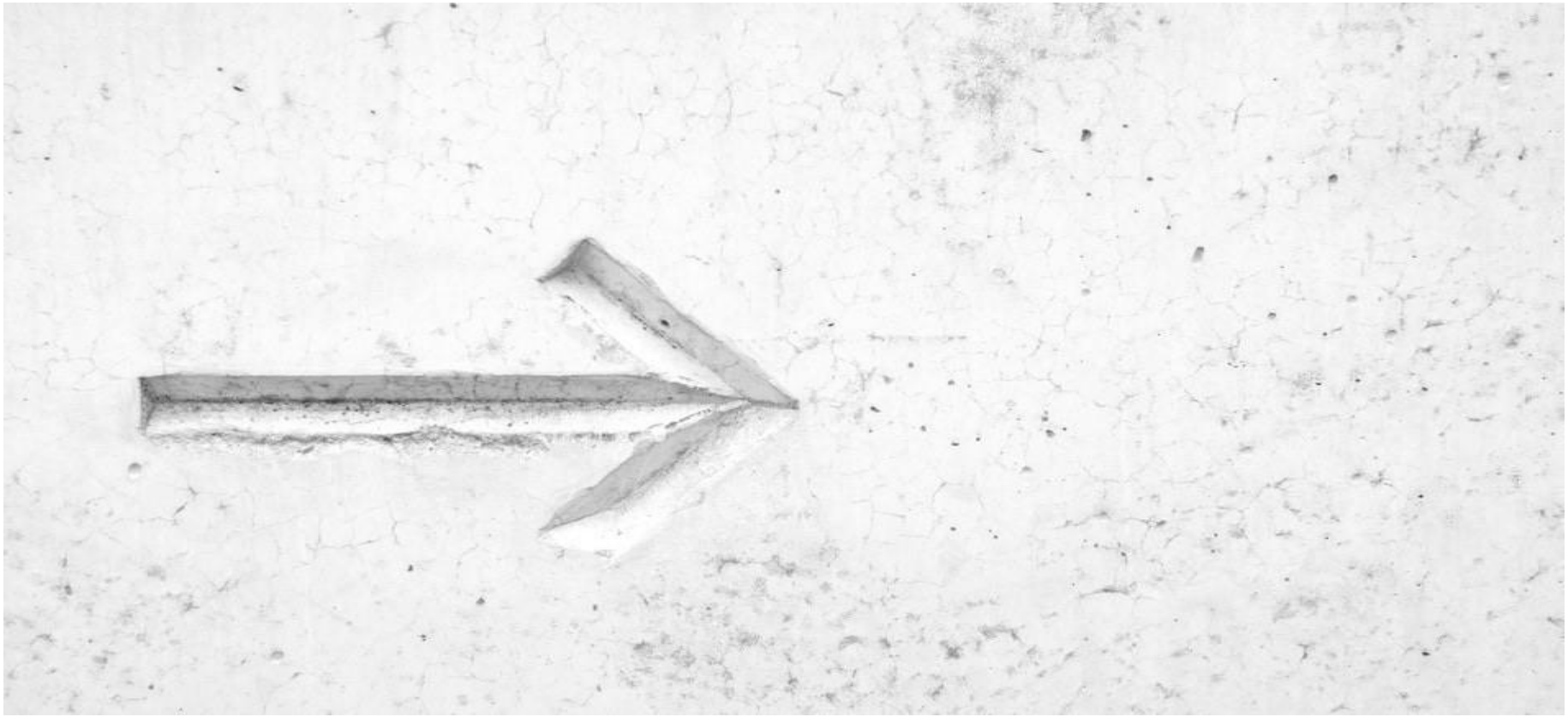
There would be a lot of people who could not afford to do this. I think user pays is not a great idea. Dunedin, general public, under 40 years, male

Key insights

- There was little support for the ecosystem concept with most unable to see many personal benefits. Negatives were much more emotively outlined than the positives. The key issues outlined were the difficulty to develop and make such a system work, discomfort with commercial entities accessing information held by government, maintaining security of the information, and potential to erode privacy and civil liberty.
- Concerns would be difficult to overcome as the concept was seen to be entering dangerous territory where citizens would lose any sense of control of their personal information.
- To win people over, significant personal benefits would need to be clearly conveyed and extensive reassurances outlined.
- An ecosystem limited to government agencies could be a first step that people would be more open to. The government was generally seen to work in the best interests of New Zealanders, although Māori were less convinced of this and would need additional reassurance.
- Nearly all participants believed there would need to be different rules in place for government versus commercial users of information, with stronger restrictions in place for commercial enterprises.
- Most felt that the ecosystem would be paid with taxpayer funds. This was another reason not to proceed as many could see more important areas they would like to see taxpayer funds spent on.
- A user pay system where consumers pay was not endorsed as it was seen to penalise low-income households. There was a general feeling that organisations that used the information should pay the costs.

Te Tari Taiwhenua
Internal Affairs

Conclusion



UMR

Conclusion

- To get people to support any of the concepts there needs to be clear articulation of the personal benefits. Currently, perceived benefits were weak, apart from for the healthcare scenario.
- People were destabilised by the perceived loss of control of their personal information – and a centralised ecosystem and government proof of identity are likely to increase the sense of loss of control.
- Commercial enterprises were seen to focus on their own interests and people would be reluctant to see them have access to personal information held by the government.
- The key potential benefits for information sharing were:
- The need to keep up with the rest of the developed world
- Better personal outcomes (mainly in relation to healthcare, possibly targeting services and government support)
- Cost efficiencies (mainly in relation to the government and the health system)
- Streamlining processes
- Better security of data
- Identifying criminal behaviour.

Document 3

Digital Identity Research Report

Brief

AATEA was tasked with undertaking focus groups to gain understanding into the relationship some Māori groups have with their digital identity. Three separate focus groups were held with rangatahi Māori in Te Whanganui a Tara (Wellington) and Te Wairoa, and professional Māori in Te Whanganui a Tara. The focus groups were held on the 9th and 13th of December, 2019. Each focus group engaged with six to eight participants from various ages, occupation and iwi groupings.

Methodologies

Prior to the focus groups, 18 forum questions, each sitting under one of several core themes were curated to guide facilitators and provide consistency throughout the three focus groups. During each focus group, the facilitator began by prompting participants to express; “what does digital identity mean to you?” This provided a foundation from which the remainder of the focus group would build on with guidance from the original forum questions.

This approach allowed our researchers to follow the provided structure of the forum questions while retaining a sense of fluidity and wānanga between facilitators and participants, and vice versa. Furthermore, this meant that discussions were lead by participants but guided by facilitators, thereby allowing participants to focus on what they deemed most significant or concerning.

Forum Questions:

What is digital identity?

Rights:
What does digital identity rights look like?
What could it look like?

Trust:
How can people use your digital identity?
Who can use your digital identity?

Safety:
What’s protecting your digital identity?
What measures are put in place to protect your digital identity (if any)?

Māoritanga:

What is the relationship between your digital identity and te ao Māori/our Māori identity?
How does being Māori affect your digital identity?
Is tikanga a concern in the movement/flow of digital identity?

Tiriti:
Is digital identity a 'taonga'?
Do you want tino rangatiratanga/sovereignty over our digital identity and if so, how do we see that materialising?

Ownership:
Do you own your digital identity?
Who owns your digital identity?

Personal:
What does your digital identity look like?
How is your digital identity influenced by being a member of a whānau/hapū?
How does your digital identity impact on collectives (whānau/hapū/iwi)? What does the digital identity of your whānau/hapū look like?

Isolated Group Themes

Over the span of two hours, participants and facilitators undertook wānanga to discuss various topics promoted by 18 forum questions. From that discussion, the following six key themes emerged:

- Ownership
- Compromise
- Privacy
- Identity
- Accessibility and Equity
- Trust and Intention

The above key themes emerged as a result of the culmination of discussions from all three focus groups, however, distinct themes within each group have also been identified. For the professional Māori respondents, the topic of informed consent was of major concern. This was particularly in regards to the ethics of physical data such as blood samples, because of the inherent mana and whakapapa it contains and the impact of such samples on a collective identity such as whānau, hapū, or iwi.

Informed consent was also topical in discussions by Te Whanganui a Tara rangatahi who expressed the relationship between informed consent, and the compromise made by consciously

engaging with social media platforms and other applications. This group also focused heavily on aspects of privacy and safety on a predominantly individual level.

Finally, Te Wairoa rangatahi also expressed privacy and safety to be major concerns, mainly in relation to personal information. Differing from the latter respondent groups, Te Wairoa rangatahi also discussed digital identity relational to self curation, as well as individual and collective reputation.

Implications for the Department of Internal Affairs

As we see the decentralisation of services, underrepresented demographics such as Māori and rangatahi have become disconnected with their data and are becoming increasingly concerned over their digital rights and security. Te Whanganui a Tara and Te Wairoa focus group participants expressed the need to build trust and clarity regarding ownership and use of their digital identity by the Government and corporate entities.

For the Department of Internal Affairs, this clearly demonstrates a demand for meaningful engagement and relationship building with Māori and rangatahi Māori. This would counteract the facelessness that can prevail in the digital age between governments and people. There was a low awareness rate regarding what roles and control the Department of Internal Affairs has concerning people's data, highlighting a need for more face to face engagement with people to inform proactive design of systems, services, and processes.

Committing to Te Tiriti as a guideline to supporting Māori rights over data as taonga is essential to serving Māori and rangatahi Māori. The ways in which tino rangatiratanga can be tangible was an overarching theme throughout the focus groups. For the Department of Internal Affairs, these focus group discussions provide a wide scope of how these groups perceive their relationship with digital identity. It is evident that much work remains in order to gain a deeper understanding further into Māori demographics and to curate new ways of operating which can serve both tangata whenua and the Government.

Recommendations to the Department of Internal Affairs

The following recommendations are made from a rangatahi Māori perspective and represent tangible actions for the Department of Internal Affairs,

We recommend that the DIA:

- in conjunction with relevant government departments, design methods of education regarding digital identity and safety to be implemented within vulnerable groups such as youth, rural and the elderly.

- design and conduct a public awareness strategy to increase public awareness and trust around DIA. Particular focus must be made on rural communities and minority groups, however, implementation generally in Aotearoa would also be of great importance.

- build relationships with rangatahi and professional Māori to gain meaningful input for the betterment of such a strategy, and become DIA's business as usual, generally. Further focus groups or engagement meetings would support this.

- take user experience (UX) of these groups into further consideration when designing platforms and services. This may look like the creation of collateral assets, for example, video or picture content in place of terms and conditions in order to increase accessibility and clarity.

- increase cultural competence and decolonisation training for staff and contractors in roles of design and user experience in particular, but throughout the organisation over time.

- assume the role of kaitiaki over data, as opposed to the owner. Participants were clear, their data belongs to them, their whānau, hapū and iwi. Assuming the role of kaitiaki would allow DIA.

Key Themes - Discussion

Ownership

An immediately evident concern and theme throughout the three focus groups was that of ownership and mana. As conversations regarding ownership commenced, it was clear that participants identified Governments and businesses as those currently owning most data. Moreso, the focus groups stated that they do not feel their data is safe in the hands of the Government. Amongst Te Wairoa rangatahi, there was a feeling of inevitability associated with the resignation of control over data. This was in contrast to respondents who reasoned that data belongs to the person or people who provide it; "Our whānau and hāpu are our original iwi. They should control our data."

Practice of data sovereignty was a significant concern to both rangatahi and professional Māori. While complete answers as to who or how data should be held while maintaining sovereignty were not agreed on, all agreed that neither the Government nor one government department

should have ownership over Māori data. One participant suggested that “wholeheartedly trusting communities and people is more powerful”, stating that a reciprocal trust dynamic between communities and governments is necessary for ethical data governance.

Participants were also asked if they considered their data as taonga under the mana of Article II of Te Tiriti o Waitangi. While the majority stated yes, one Te Whanganui a Tara rangatahi stated no, saying; “I feel for me, my data isn’t my own. It loses its mana once I give it to the government and nothing’s ever safe.” This suggests that what defines a taonga to an individual is autonomous control and ensuring it's safety, kaitiakitanga. Another participant stated that “whoever owns the data, maintains it”, supporting this conclusion.

Compromise

The prevailing theme of compromise was recognised by participants as an unavoidable aspect of using personal devices and digital platforms. Personal security and individual ownership of data were main participant concerns about sacrificing autonomy to have access to online services and applications. Popular social media platforms were considered by rangatahi focus groups to be selling their personal information to third parties to form effective targeted content and advertisements, based on patterns in search history and data gathered through device surveillance.

Rangatahi from the Te Whanganui a Tara focus group stated: “If I want to be on social media or I want to have access to my friends through my phone, I have to forgo some personal security.” The means by which many applications are able to access this personal information legally is through terms and conditions agreements. This was viewed by Wairoa rangatahi as “the box you’re allowed to play in”. Terms and conditions are necessary to agree to for access and were seen by participants as being filled with jargon and rarely being comprehensive, accessible or understandable, relative to their capacity to be so.

“If they wanted to make this stuff accessible and useful for the consumer, they so could. It’s so easy to use everyday words now.”

Rangatahi expressed that to know what was happening to their data, they relied on sources outside of terms and conditions agreements. In making this information accessible, rangatahi expressed that their relationship to their personal devices and applications may be different. “The more I learn about what I’m sacrificing, the less I want to sacrifice.” Terms and Conditions agreements were seen by participants to be an avenue to provide legal protection for businesses, as opposed to tangible protection for the rights of the consumer.

The selling of data to third parties was recognised as being the main provider of revenue for popular social media platforms such as Facebook. Rangatahi from Wairoa stated: “If it’s free, then the user is the product” and “Your information is the product that they’re making money off of.” To

deal with the demoralisation associated with the loss of personal security, some participants went as far as relinquishing their regard of their personal data as a taonga.

“I don’t treat my data as taonga so it’s not. If I have to give all of this information to the government without having any control over it, then how can I honor something that’s tapu to me.”

An undercurrent throughout the discussions around compromise was the notion of consent, in particular informed consent. The importance of consent concerning the distribution of information was a concern to all groups and was also closely linked to the theme of privacy.
Respondents noted a lack of ethics and open communication as a vulnerability in the system and that more work needs to be done so whānau can be more informed when giving consent. The layers of informed consent were also explored, common law and tikanga being considered as foundations to consent, of which whānau must be made aware of.

Assumed consent was also of concern. For examples, photo sharing without prior notice given to subjects within the photo being shared; “The threat to privacy and data sovereignty isn’t only through technology or this digital world, it is also through people.” This normality of assumed consent and awareness of the permanence of the internet was expressed as another concern. Rangatahi in Wairoa identified that it is difficult to remove information or photographs once they have been uploaded, and that information is stored permanently. This led into discussions of self representation online in a way which honoured the identity and interests of the groups they were apart of such as whānau, school, and community, particularly concerning tagged photos online. This is evidence that these rangatahi are conscious that their online identity can have significant effects on their future and the reputation of themselves and communities.

Privacy

The statement: “Nothing’s ever safe, nothing’s ever private.” was the general consensus among participants concerning the status of their shared information, data, and activities while in the proximity of personal devices. Surveillance, targeted advertisements, and data security were key talking points for participants under this topic.

In regards to surveillance, there was an assumption among rangatahi in Te Whanganui a Tara that it was common knowledge that constant surveillance is occurring through our personal devices, through application access to location services, microphones and cameras. This awareness is prevalent in popular memes and has influenced the behaviour of participants, as the constant awareness of monitoring causes some to remove their phones from private situations or discussions, and covering front cameras on laptops and phones. This shows an inherent lack of trust toward entities who collect others’ personal data.

A general feeling of apprehension in relinquishing all privacy was also evident. This is captured in this statement by one rangatahi; “I act like someone’s always watching. We just assume

someone's always watching us." The examples given here by Te Whanganui a Tara rangatahi mainly concerned their physical presence in relation to being surveilled, which in turn informed their opinions around the widespread knowledge that they are being surveilled. This was in contrast to rangatahi in Wairoa who stated that people are no longer as private, nor aware of the consequences of sharing their personal information, or concerned about it, due to the ease by which data can be distributed. Wairoa rangatahi also stated that security measures could be taken to protect individual privacy such as end to end encryption, with some presuming that commonly, rangatahi are aware of these measures. However, there was an awareness that the relationship to data and digital identity held by people who use digital platforms in a professional capacity, can differ greatly to those who may use it solely for personal reasons.

Targeted advertisements were another concern for participants, one stating that, "Social media are some of the most powerful marketing tools ever. I just think about how I can keep myself safe." Concerns around the prevalence of algorithmically monetizable content that is constantly streamed in the form of suggested content and targeted advertisements were raised. The rangatahi noted the formation of a personalised online landscape or "echo chamber" on social media platforms as an example. This was seen to have a profound effect on how an individual perceives themselves and their identity. It was considered to be intellectually stagnating rather than challenging. It also limited an individual's opportunity to profoundly explore a myriad of interests and opinions, relative to the seemingly endless amount of content that exists online. This reflects inherent biases instilled in the online landscape.

"I'm very much aware that if I look at something on google, I can jump onto Facebook and there will be ads for it."

This concern regarding the use of data extends also to general data security in both a digital and physical sense. One example given in relation to physical security and safety was location tracking and sharing. Location tracking was discussed in relation to applications and personal device access to location services, location sharing through online photos and information containing an individual's whereabouts being accessible by the public. Digital security was also a major topic with examples such as potentially unsafe online password security keychains and scamming being mentioned.

"Our threat is privacy and safety but for my Aunty her threat could be scamming."

Identity

In discussions of digital identity, multiple layers were explored beyond the realm of one's individual online presence. While online identity presence was acknowledged as being significant, a prevalent theme was the security and safety of one's physical identity which, with the progression of technology, has now become synonymous with aspects of one's digital identity. A repeatedly used example of this was DNA samples such as blood, and having ownership over such samples claimed by those collecting them, whether for medical or personal testing purposes. "Why would

I take my tīpuna, why would I take the blood that holds all of our tīpuna, and send it to another country?" This also initiated discussions regarding tapu, noa and how the lines are becoming increasingly blurred. This correlates directly to the more personal data we share, especially in a physical sense. The implications of tapu, noa and mana for Māori are of high concern as physical identity was seen to extend into collective identity. This also relates to participant conversations around data as a taonga, and ties into whakapapa and collective data ownership.

Throughout discussions of personal, physical and collective identity, the overarching concern and awareness was the indelibility of such information once it reaches an online or digital platform. Rangatahi from Wairoa stated that for personal protection: "Don't post anything you don't want to see on the front of the newspaper." This tied into discussions regarding both personal and collective identity as a means of representing people and groups. Therefore, while serving as a tool for self-curation and profiling as an extension of one's self, in some circumstances, one's digital identity can also be ill-represented or manipulated by others. As one person stated, "I hate it, I never put my ethnicity down" highlighting concern over how their data is used and what it is used for. Additionally, as one Māori professional expressed, "They know who I am but I don't know who I am!"

Accessibility and Equity

With the collection of data being a concern to participants, access to data was considered as similarly significant, and that easy access for whānau to whānau data is crucial. A major example regarding this discussion of accessibility was the RealMe platform and the 2018 national census. In the different focus groups, respondents stated their frustration with platforms like RealMe as overly confusing and not user friendly, unless you had access to someone who had previously been through the process. Next, the failings of the 2018 national census was well known throughout focus groups with participants from predominantly minority populations expressing concern. "Our whānau don't always have a voice." This lack of voice was mainly attributed to a lack of connection and accessibility between census organisers and rural communities in particular. One rangatahi stated, "If they're going to roll out a digital platform then they have to make it so everyone who needs to use that platform can. If they don't have access to the internet or a device, then they're shutting them out from the start."

With this acknowledgement of disconnection between some communities and officials involved in data collecting, digital identity creating platforms were presented as an opportunity for communities. Participants explored concepts of online community spaces as an avenue for connection and communication. Another opportunity presented was digital identity education to assist people in connecting and safely navigating digital spaces; "How do we incorporate this into our education system and into our curriculum to be able to teach our rangatahi and pakeke how to actually think critically and be discerning?"

The participants identified that another topic of particular concern for Māori is the inherent eurocentrism of data collection and implementation, namely by the Government. The basis in Western belief systems and their historically-informed risks presented to Māori was discussed. One participant stated that: “There’s a massive risk if you’re indigenous cause there’s racial profiling on everything. That’s where we need to find trust and relationships with our Government and DIA to make sure they have our back.”

Another concern voiced by participants is the unconscious and conscious biases imbued in government processes, evident also in technology creation. One rangatahi said “What is our first choice going to make and who does it benefit? It’s never Māori unless it’s a Māori business”. This supports the notion that should empathetic consideration not given to diverse groups then products, services or platforms will not be user friendly.

Trust and Intention

Finally, trust, or lack thereof, was presented as a principal concern by participants, particularly in relation to the intention of data use by those holding data. This was applied to companies such as social media platforms, technology companies and businesses in general. However, this distrust of data collectors extended past technology and social media companies to the Government and the Department of Internal Affairs. In response to this distrust, participants highlighted the need for honest communication and trust from the Government in communities as avenues to build trust in the Government and DIA. As one Te Whanganui a Tara rangatahi stated, “In order to create an environment where we have trust in those holding our data, they need to also have trust in us.”

Understanding the intention behind Government stored data was also discussed. One participant explained that they would have greater trust if they knew the purpose for their data being collected. This was further developed in discussions regarding the constant need to supply data, with participants unable to identify the purpose of collection. One participant said, “They’ve got it all, why do they keep wanting it - I’ve got no more to give.” Te Wairoa respondents explored the relationship between trust in giving data and the avenue of which said data is being collected. For them, this looked like having recognisable figures and faces engaging with them directly in order to maintain accountability.

This sense of distrust in intentions was attributed by respondents as being a result of historic misuse and abuse of Māori data, creating biased and incorrect assumptions regarding Māori and other indigenous peoples. “There’s so much kōrero that needs to be had on indigenous trust in Government because of how they’ve used and abused our data in the past”. Another said, “Who keeps them honorable?”

Yabble

The place where brands meet fans

Project Services

Insights Report

June 2019

Background to This Presentation

- The New Zealand Government is currently looking at digital identity rights, inclusion, economy and algorithms
  - This work is spread across multiple agencies, and is **specifically looking to understand from a citizen perspective perceptions and experiences with digital identity in government services**
  - This work is being led by the Digital Identity Transition Team in the Department of Internal Affairs (DIA)

- This presentation shares the results of the Project Services research
  - Survey conducted 27th May to 4th June 2019
  - Total of N=527 completes

Sample Profile

GENDER

Male	50%
Female	50%

AGE

18-24 years	7%
25 -34 years	20%
35 - 44 years	18%
45 - 54 years	21%
55 - 64 years	17%
65 - 74 years	13%
75 years or over	4%

ETHNICITY

NZ European	73%
Maori	7%
Chinese	6%
Indian	5%
Pacific Islander	2%
Other Asian	3%
Other Ethnicity	5%

HOUSEHOLD

Younger couple / Single	20%
Younger family	25%
Older family	25%
Older couple / Single	30%

REGION

Northland	3%
Auckland	38%
Waikato	8%
Bay of Plenty	8%
Gisborne	<1%
Hawke's Bay	3%
Taranaki	1%
Manawatu-Wanganui	4%
Wellington	10%
Nelson	<1%
Tasman	1%
Marlborough	1%
West Coast	1%
Christchurch	13%
Canterbury	4%
Otago	4%
Southland	2%

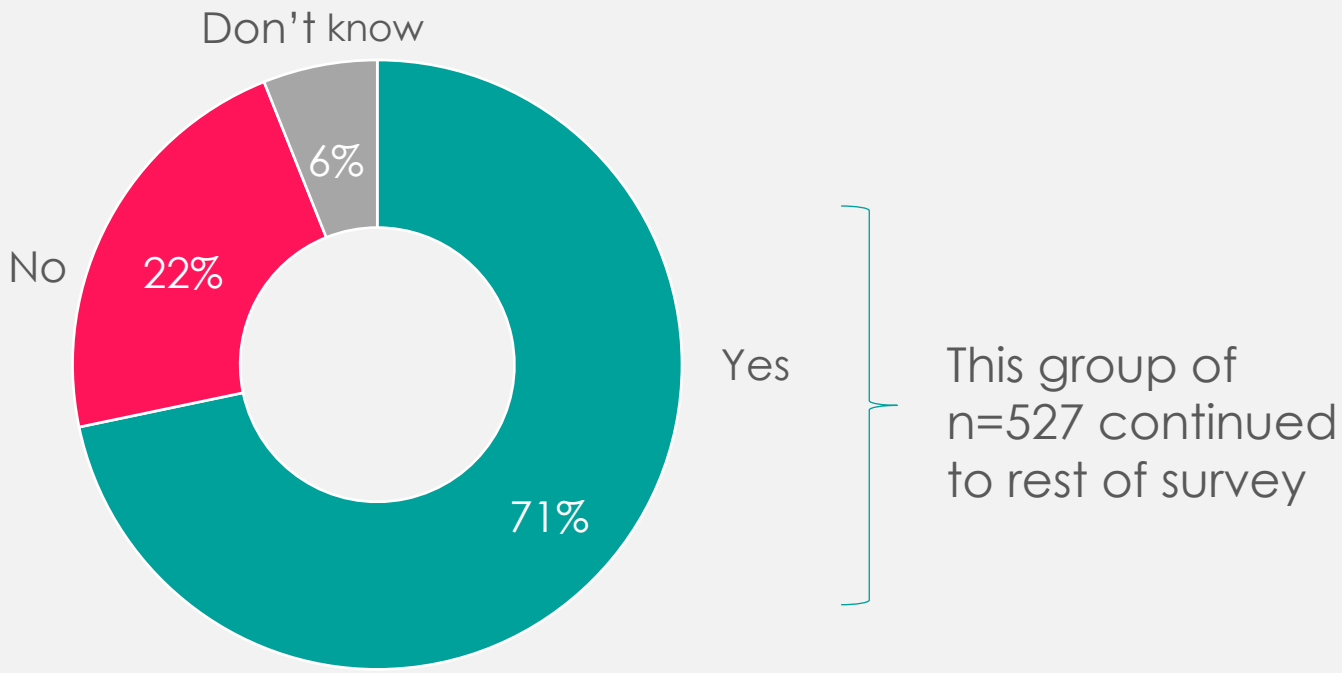
Base: Total N=527, must have used government services in the P12M

Yabble

Results

7 in 10 citizens had used a service by a government department that required proof of identity in past 12 months

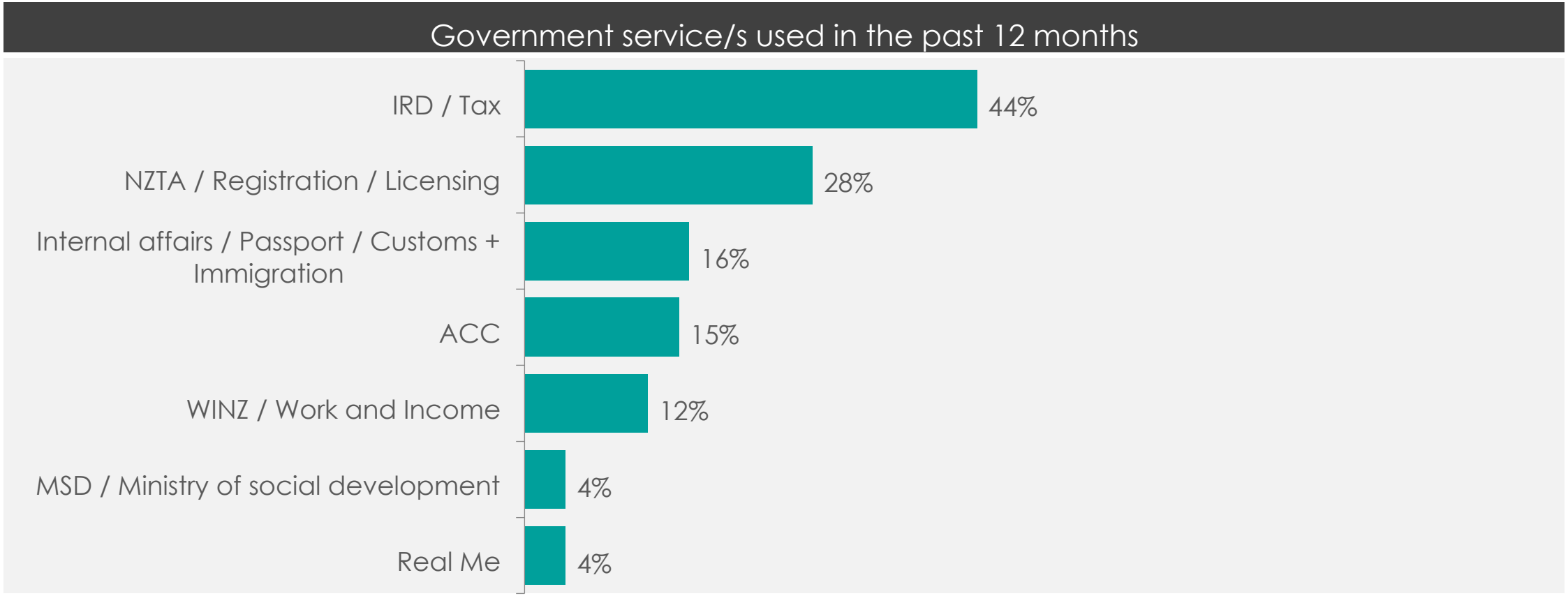
Used a service provided by a government department or agency which required proof of identity



Base: Total Sample N=742

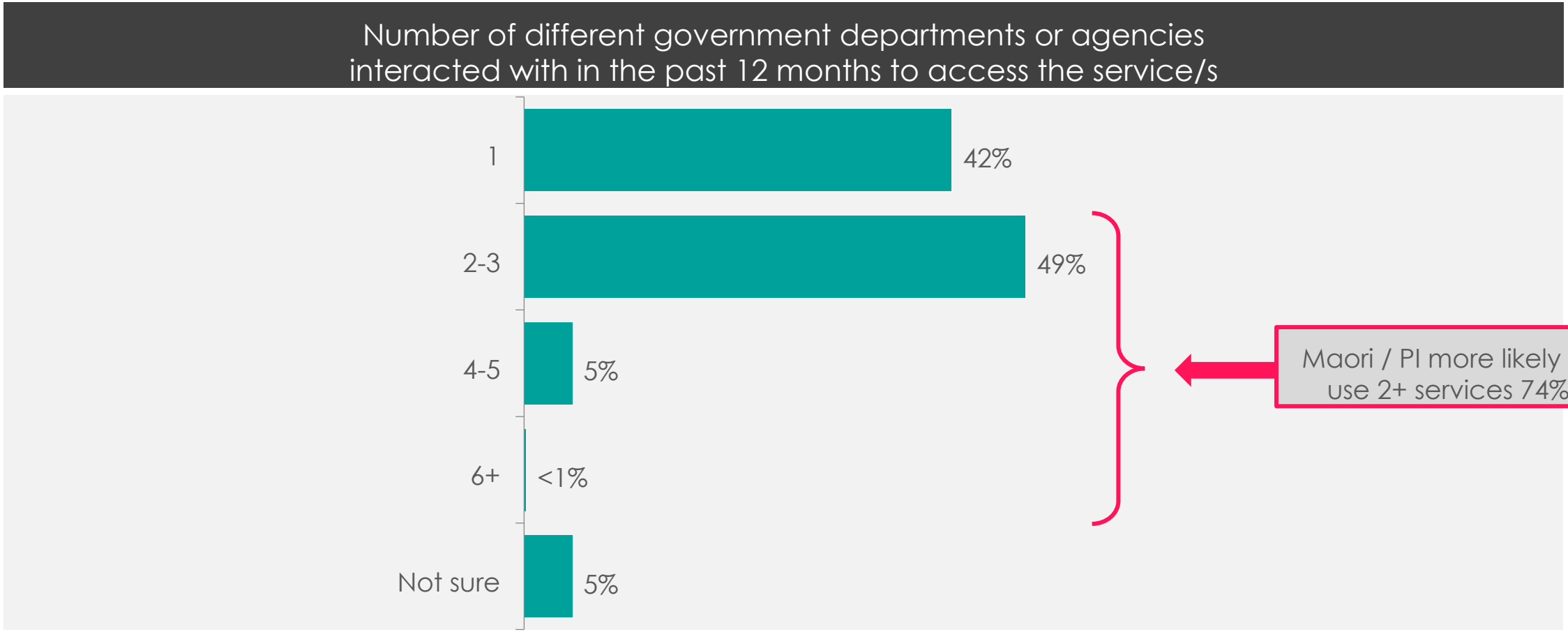
Q: Have you used a service provided by a government department or agency which required you to provide proof of identity, such as your name, date of birth, or gender in the last 12 months? For example, registering a vehicle, filing a tax return, or applying for accident cover through ACC.

Main types of government services used included IRD / Tax and NZTA licensing



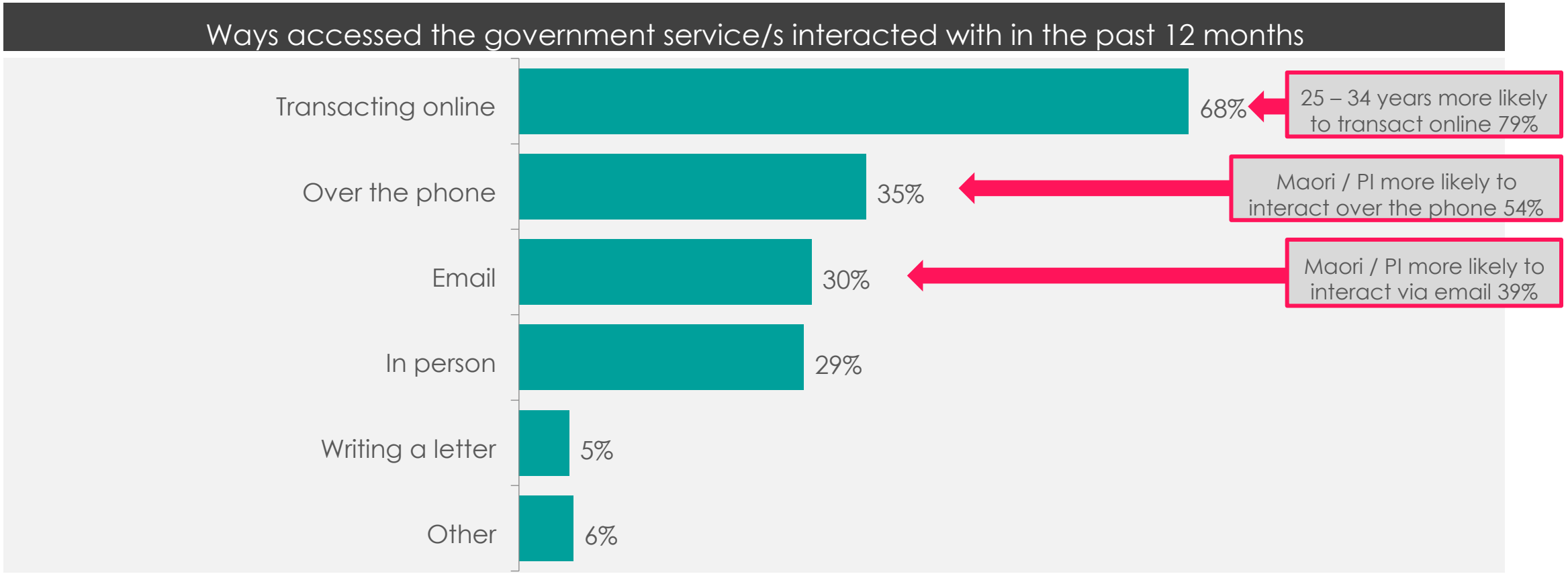
Base: Total N=527
Q: Which government service or services have you used in the past 12 months?
Other mentions include (<1%): Dept of conservations; Parental Leave, Healthcare, Hospital, Ministry of Justice, BDM, EWRB

Those who have interactions, generally deal with between 1and 3 agencies in a 12 month period



Base: Total N=527
Q: How many different government departments or agencies did you interact with in the past 12 months to access the service(s)?

With access to government services predominantly done online, especially among those under 34 years



Base: Total N=527

Q: In what ways did you access the government service(s) you have interacted with in the past 12 months?

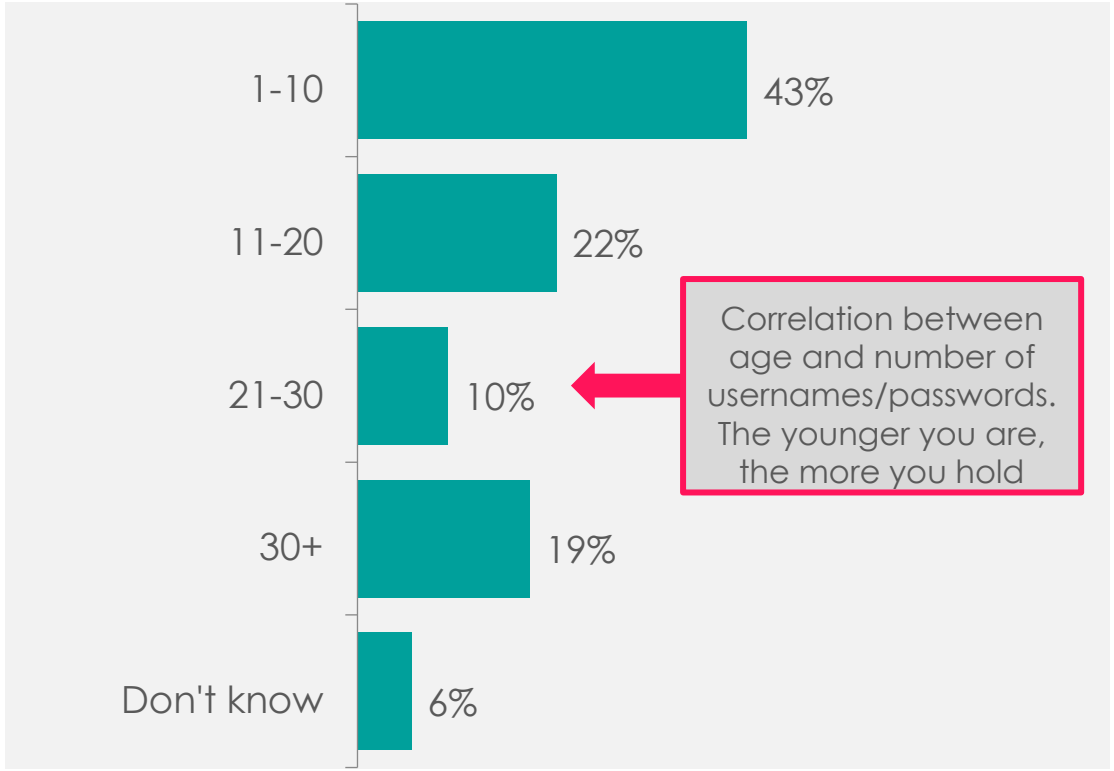
Online Context for Digital Identity

Beyond just Government Services

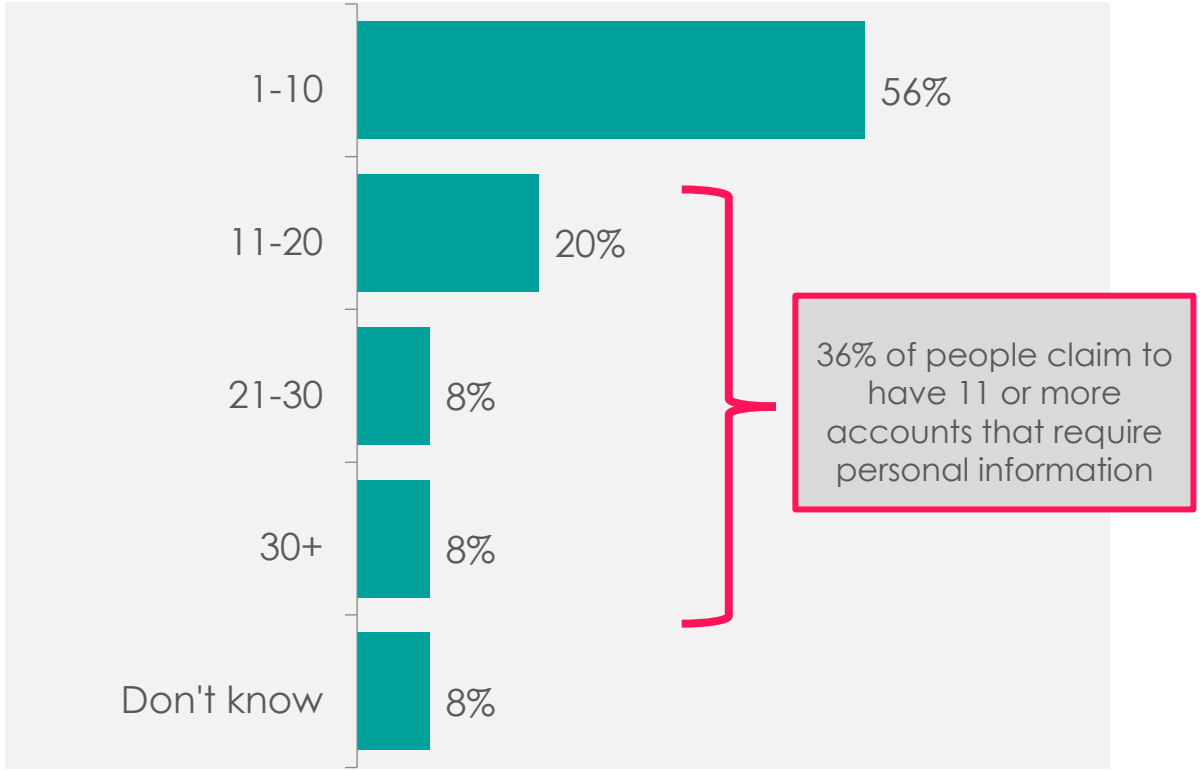
Yabble

It is common to have a multitude of online passwords and usernames, particularly the younger you are

Approximate number of online usernames and passwords have



Number of online usernames and passwords that required personal information



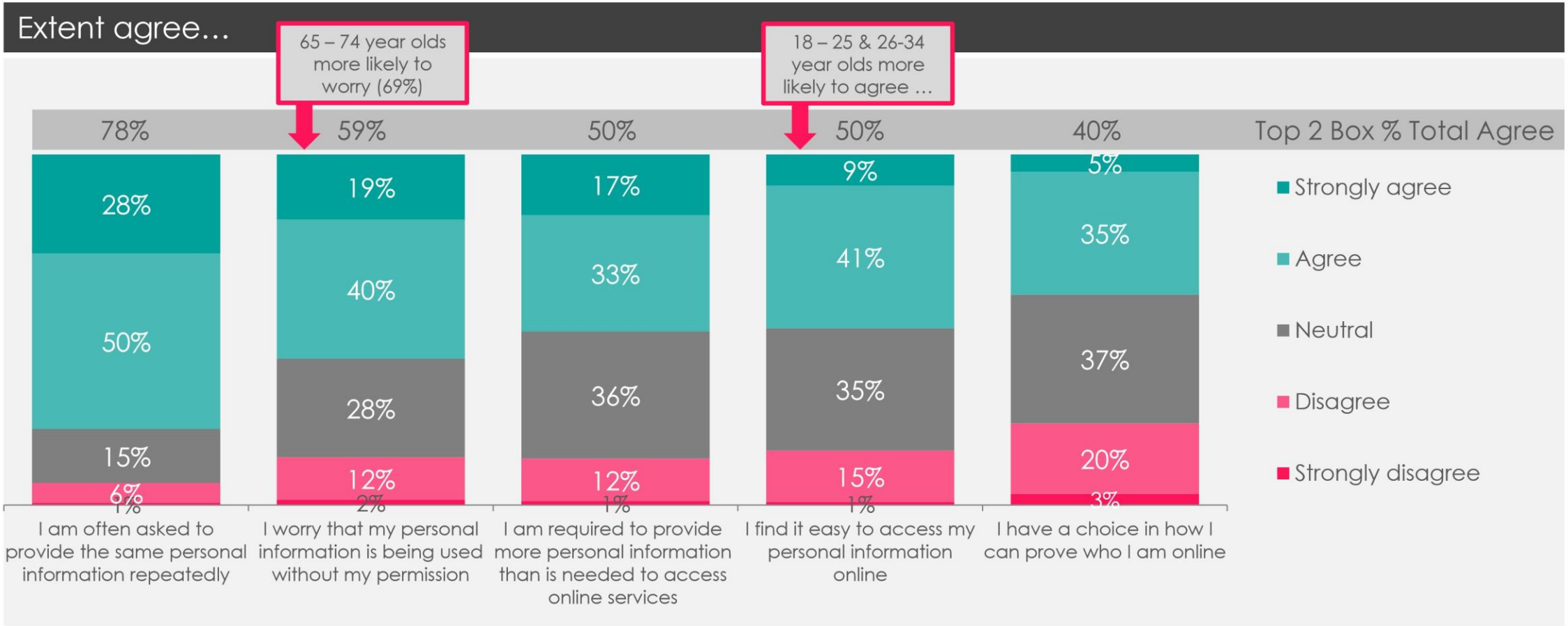
Base: Total N=527

Q: Now thinking a bit more generally about all the services you use, not just government, approximately how many online usernames and passwords do you have?

Q: How many of these have required you to provide your personal information?

Yabble

People feel that they are asked the same personal information repeatedly, with lower agreement that they have a choice in how to prove who they are online

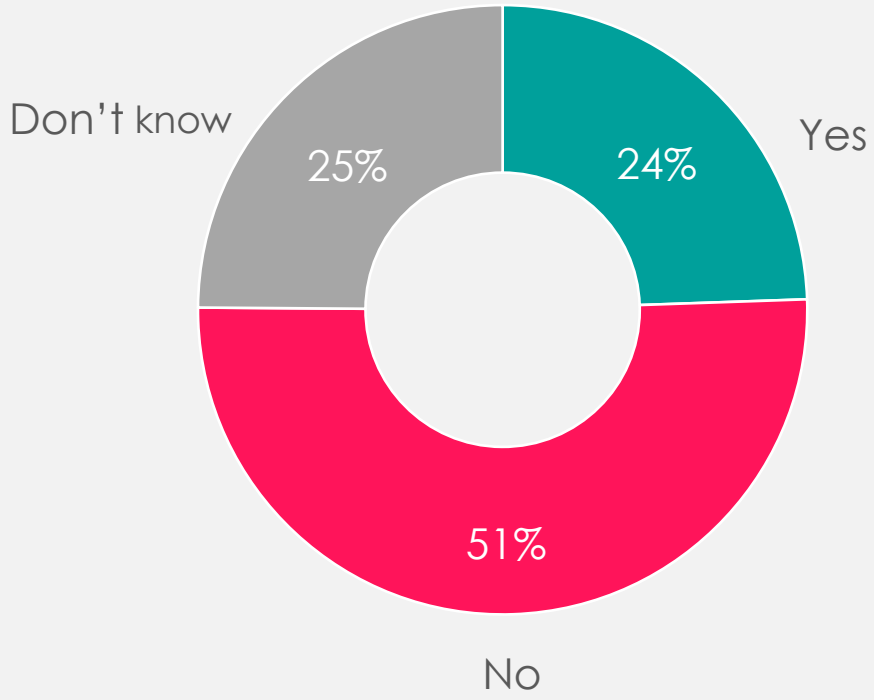


Base: Total N=527

Q: How much do you agree with the following statements?

With a quarter claiming their personal information has been leaked, hacked or used without permission in the past

Ever experienced a time where online personal information was leaked, hacked or was being used without permission

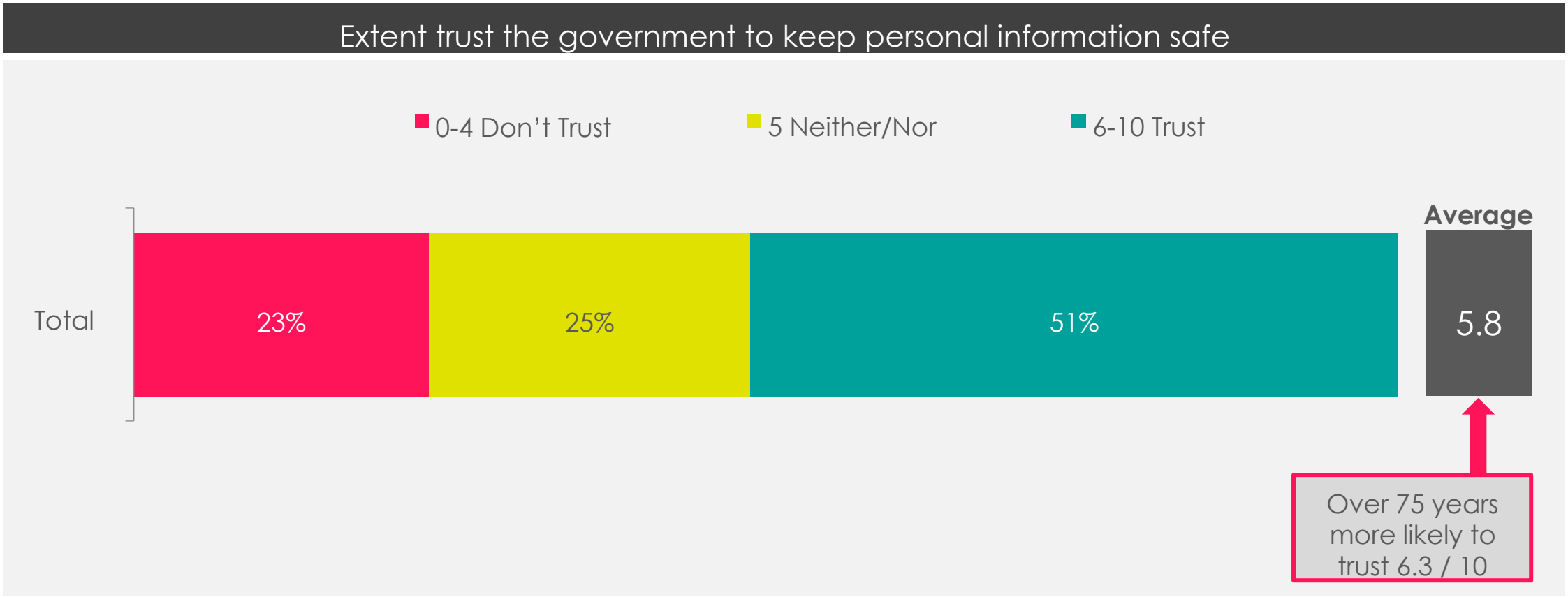


Base: Total N=527

Q: Have you ever experienced a time where your online personal information was leaked, hacked, or was being used without your permission?

Perception of Government and Personal Identity

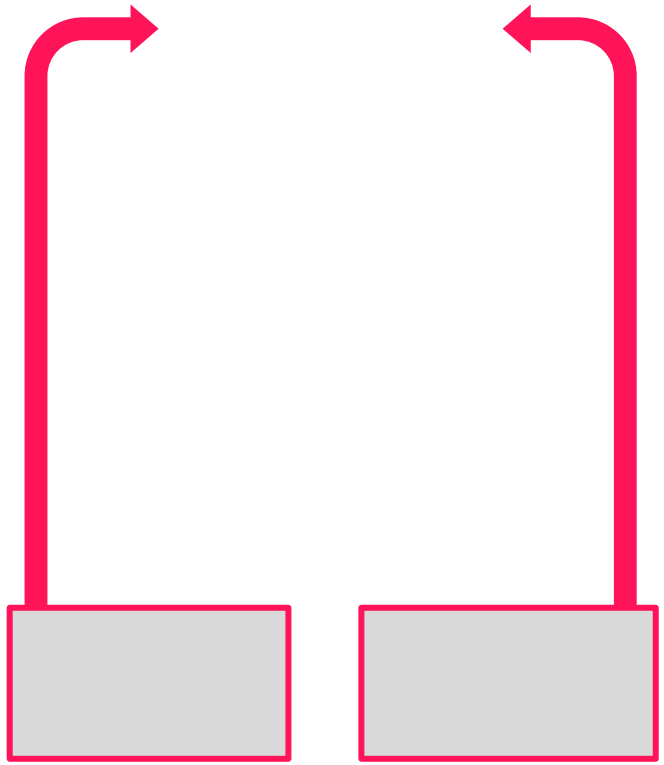
About half of the citizens included, trust the government to keep their personal information safe



Base: Total N=527
Q: To what level do you trust the government to keep your personal information safe?

Half of those who have used government services agree that the government needs to do more to protect personal information

Things the government



- **NOT SHARING INFORMATION** (50 mentions)
  - › *"Never sell to any other party. Remind us to keep it secure."* › *"I'm worried about my details not being anonymized when doing for data mining. I'm not convinced that the information practices are being followed that protect the information of users. I would want more assurances of this."*
- **SECURITY** (45 mentions)
  - › *" End-to-end encryption, 2FA enabled, encrypted databases."*
  - › *"Protecting sensitive data from hacks. Identifying and securing weak points in data shared between departments."*
- **AUTHENTICATION / IDENTIFICATION** (9 mentions)
  - › *"2 factor logins on all websites. Verification if signed in from devices, or warnings."*
- **LAWS AND REGULATION** (8 mentions)

53%*

Agree that the government needs to do more to protect their personal information

Male more 65 – 74 years likely to more likely to agree 58% agree 61%

› *"Government employees that breach privacy laws should be prosecuted as well."*

› *"Introduce more extensive laws regulating what private companies can do with our personal information online."*

Base: Total N=527

Q: Do you believe that the government needs to do more to protect your personal information?

Q: What do you believe the government should be doing to protect your personal information online?
** Made up of 30% who do not trust, 30% neither, 40% trust*

Awareness and Perceptions of Real Me

Majority of those who have used a government service recently are aware of RealMe, and over half have used RealMe. There is a correlation between age and usage – the younger you are the more likely you are to have used

80%
aware of RealMe

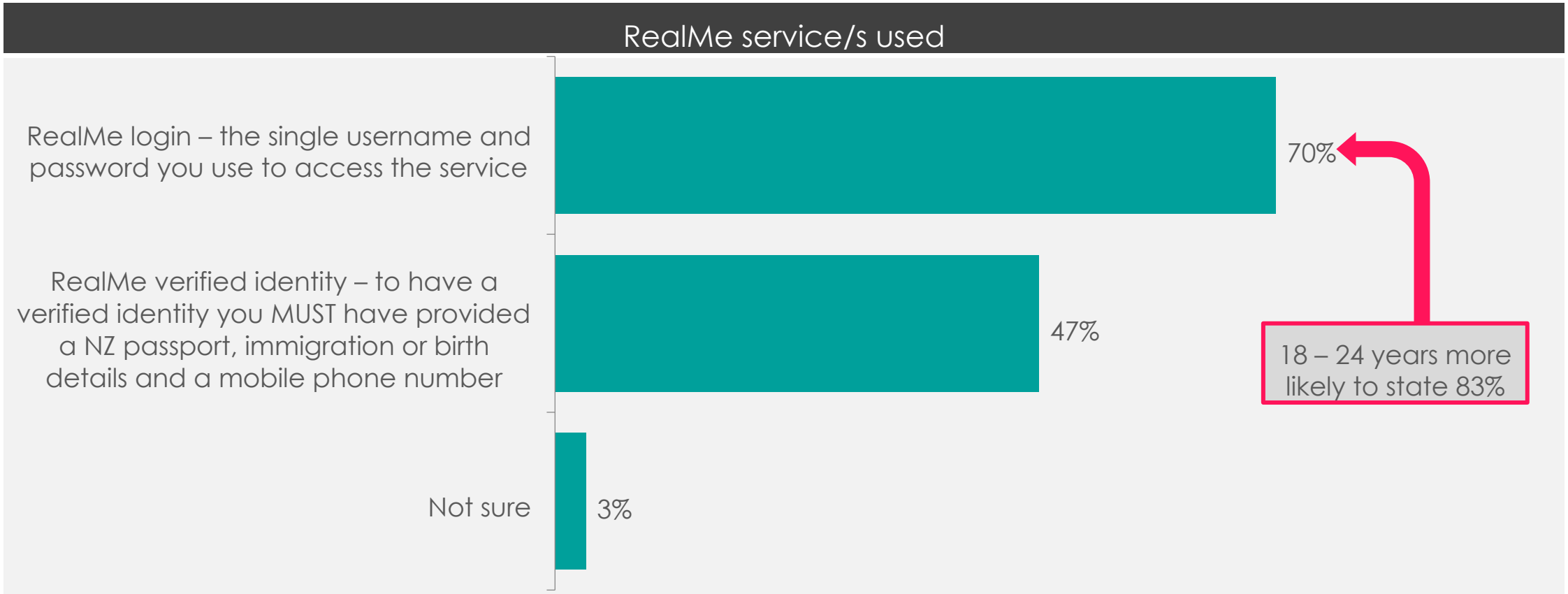
56%
Have used RealMe in the past 12 months

Correlation between age and likelihood to be aware and to have used. Younger more likely to be aware

Asian more likely to have used 65%

Base: Total N=527
Q: Before now, did you know of RealMe, the identity verification and login service?
Q: Have you used RealMe in the past 12 months?

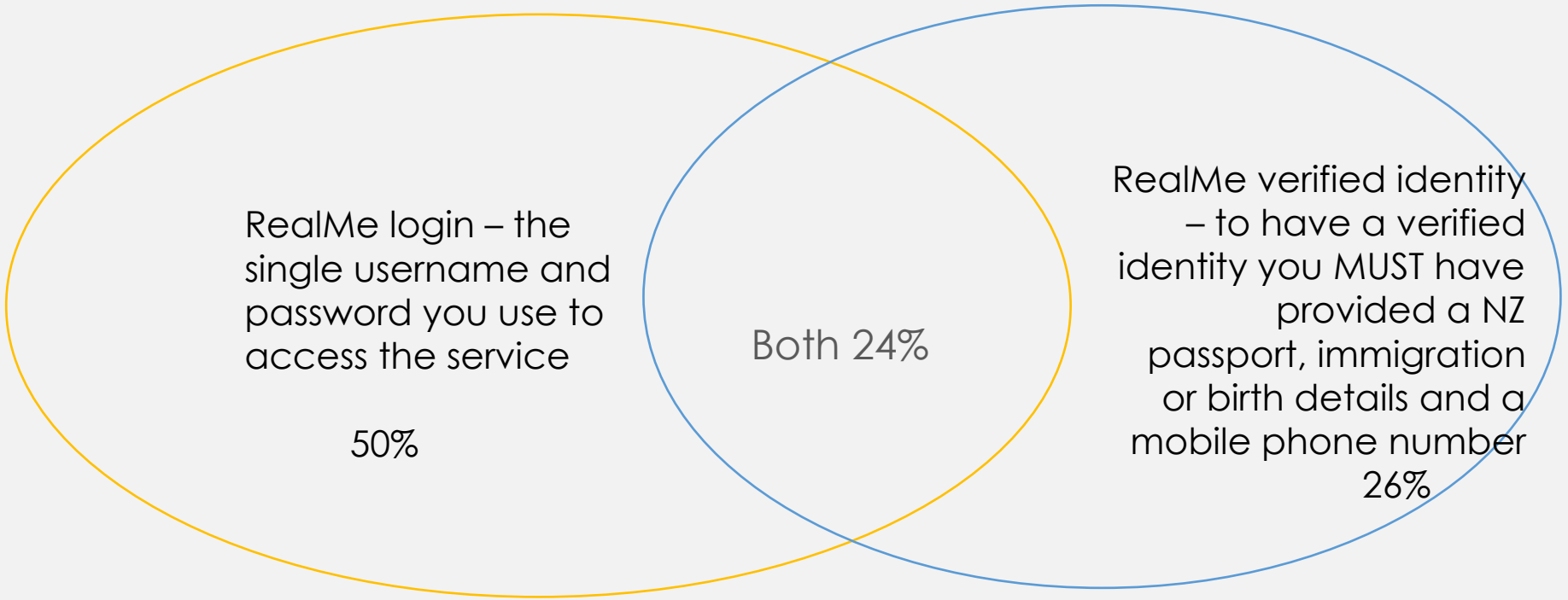
RealMe login is the more popular of the two services used



Base: Used RealMe in the past 12 months N=293
Q: Which RealMe service/s did you use?

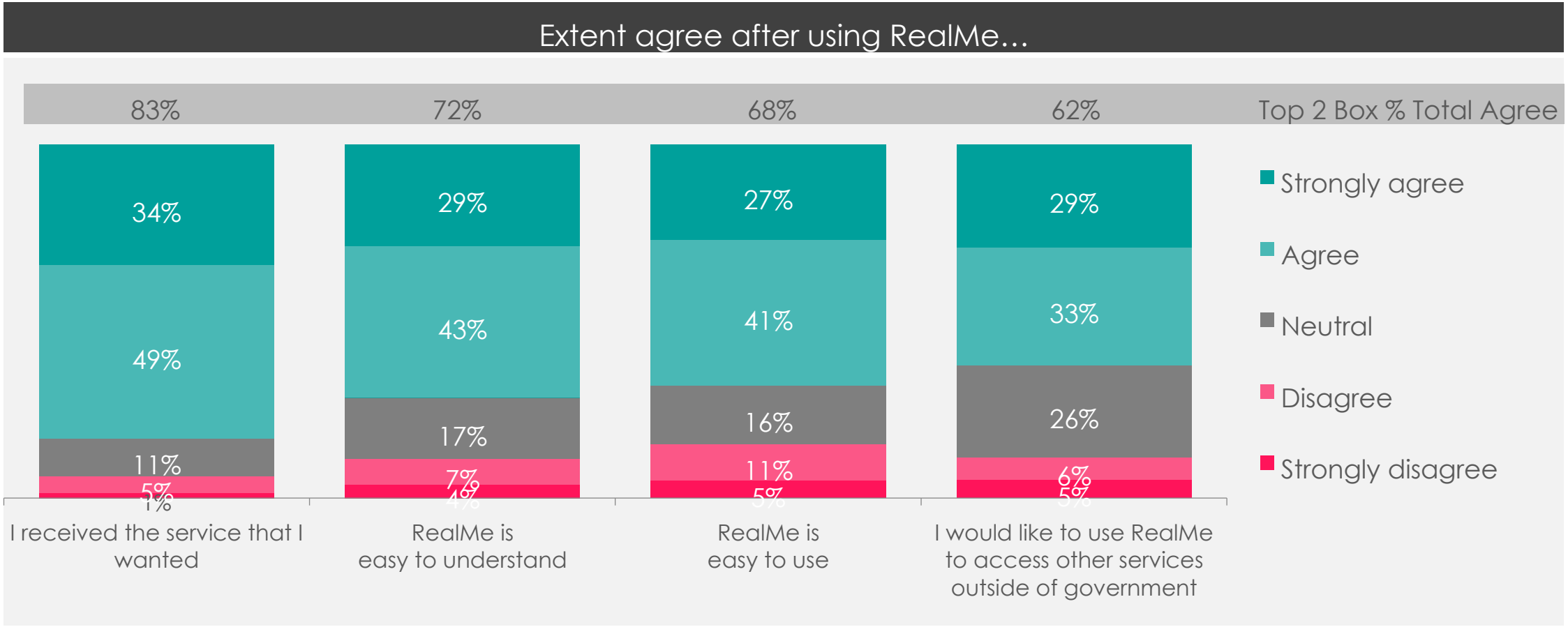
RealMe login is the more popular of the two services used, but almost a quarter have used both

RealMe service/s used



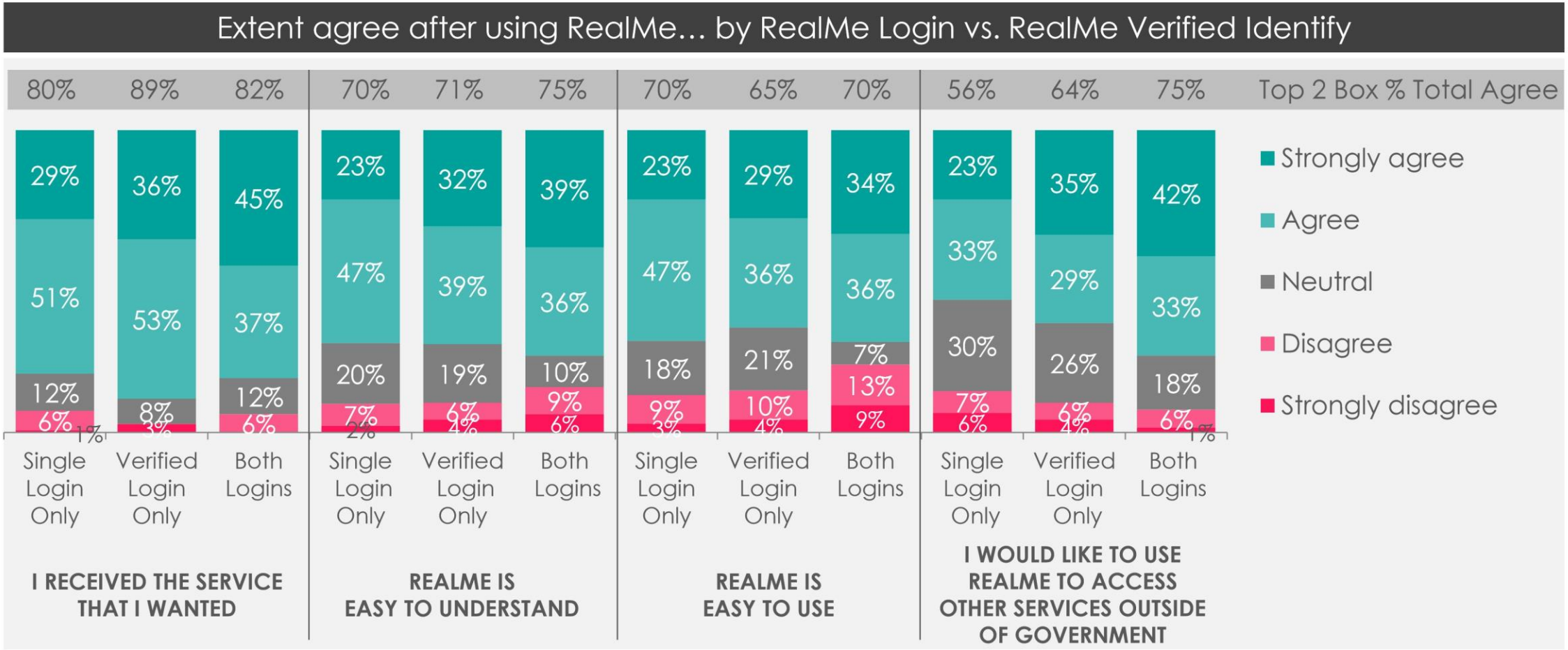
Base: Used RealMe in the past 12 months N=293
Q: Which RealMe service/s did you use?

With positive experience, acceptance and perceptions of RealMe among users



Base: Used RealMe in the past 12 months N=293
Q: After using RealMe, to what extent do you agree with the following statements?

Those having used both login more likely to use REALME to access other services outside of government



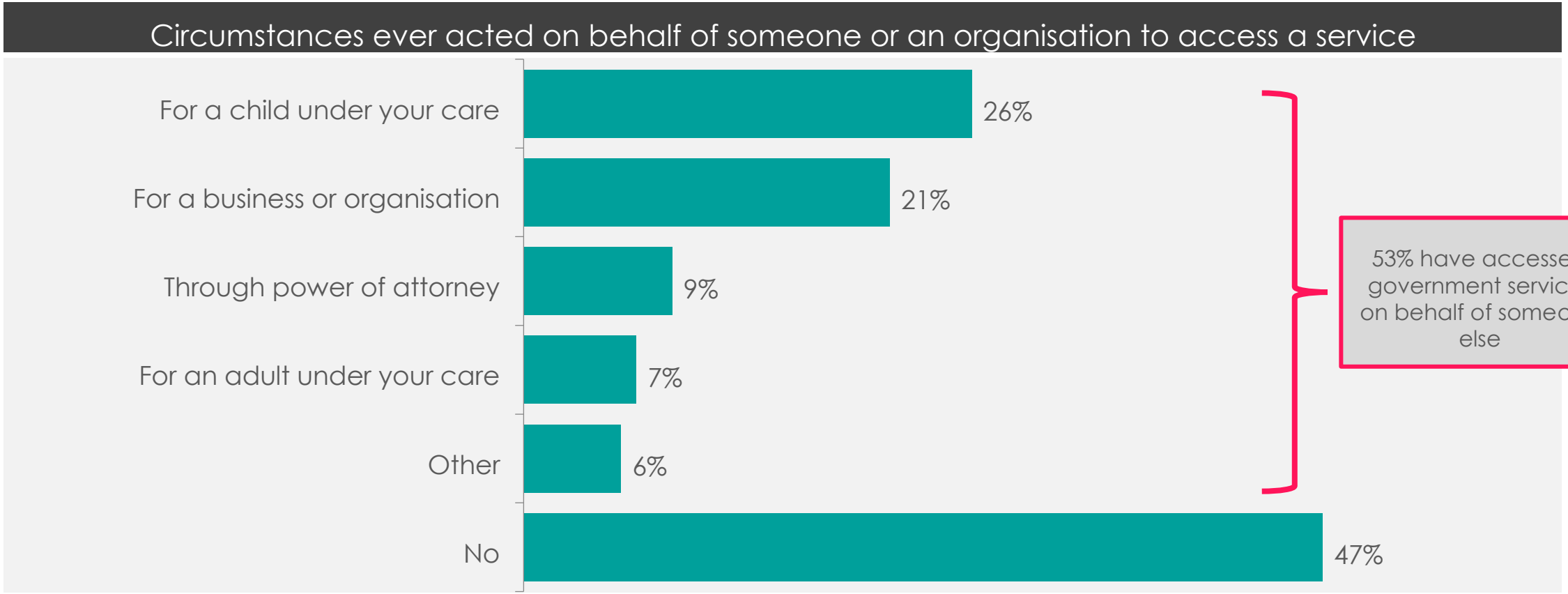
Base Used RealMe in the past 12 months: Used RealMe Single Login Only N=139, Used RealMe Verified Login Only N=72, Used Both Logins N=67

Q: After using RealMe, to what extent do you agree with the following statements?

Acting on behalf of others...

Yabble

Just over half of those who have accessed government services in the past 12 months have had to act on someone's behalf at some stage

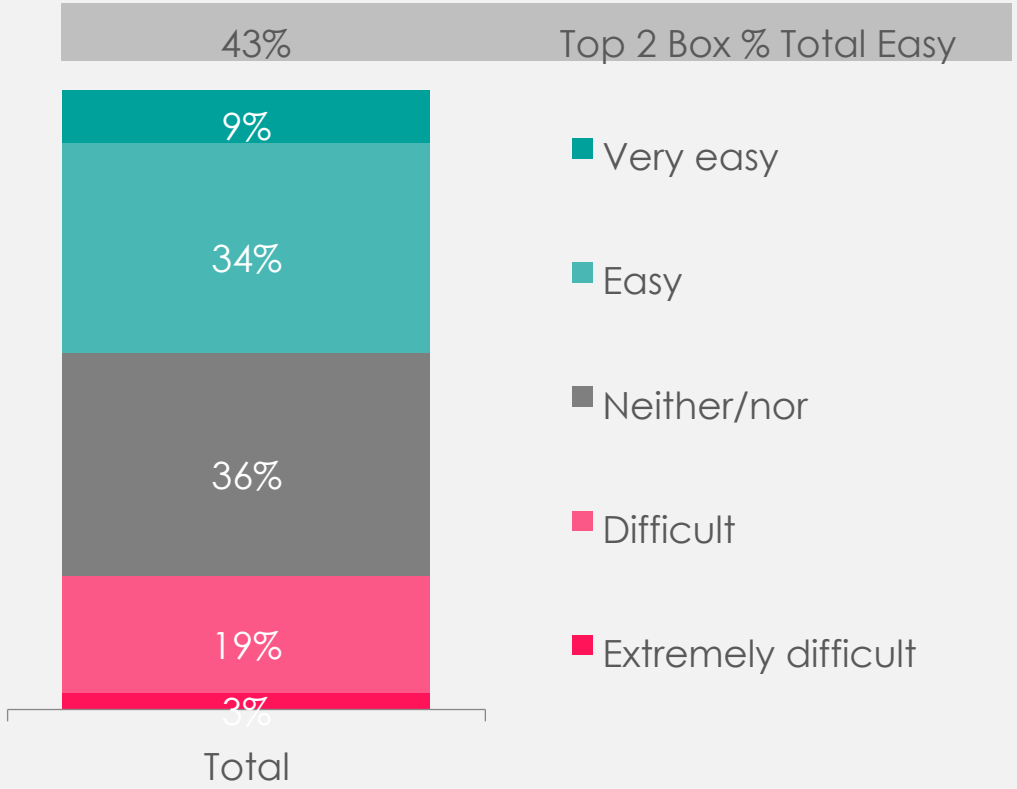


Base: Total N=527

Q: Have you ever had to act on behalf of someone or an organisation to access a service in any of the following circumstances?

Experience of acting on behalf of slightly polarised, with just over 4 in 10 finding it easy, but 22% saying it was difficult

Ease of experience acting on behalf of someone or an organisation to access a service



Base: Ever acted on behalf of someone or an organisation to access service N=259
Q: Did you find the experience easy?

Main difficulties involve getting hold of someone, establishing or proving access, or lengthy forms and paperwork

Difficulties experienced when acting on behalf of someone or an organisation to access a service

- **CONTACTING/ TALKING TO SOMEONE**
  - *"Answering questions and also just making contact over the phone without having to wait 10 minutes."*
  - *"Not enough info on website, wasn't that obvious on the site, of contact details if you had problems interacting with the website (it was IRD). Esp. finding an 0800 phone no. to contact for personal help."*
  - *"Trying to find a way out when you hit a wrong button, or the answer was not sufficient for the question.... to then try contacting a HUMAN was impossible. I gave up on three or four separate occasions."*
  - *"Idiotic automated telephone systems that will not give an option to speak to a real person - any agency/department that has those systems generally has a very poor customer approach - it is certainly not worth calling it service - and a high level of its own importance - arrogance even."*

- **ESTABLISHING / PROVING AUTHORITY TO ACCESS**
  - *"Proving that the other person wants me to act on their behalf, when that other person does not speak English, and does not live in the same area as me, so cannot come to the phone while I am trying to do the business."*
  - *"Proving that I had the right to access the data."*
  - *"My son has cerebral palsy with speech difficulty but is over 16 but the agency wouldn't let me speak on his behalf."*
  - *"Being able to prove I held authority to act on behalf - required to provide multiple copies of that verification to the same agency."*

- **FORMS / PAPER WORK**
  - *"Having to fill out forms and then being told that the EPoA trumps everything else."*
  - *"Duplicating info on forms."*
  - *"Long forms, amount of information required, repetitive questions."*

Base: Total N=527
Q: What did you find most difficult about the experience?

Yabble

Concluding Thoughts...

Yabble

Concluding Thoughts…

- Using a government service where proof of identity is required is relatively common, with 7 in 10 stating they have done so in the past year
- IRD and tax are the most common places where Kiwis have used government services, followed by NZTA / licensing
- Accessing government services is predominantly done online – with almost 7 in 10 having had an interaction this way in the past 12 months

ONLINE CONTEXT

- There is agreement that providing information repeatedly is a common issue, and there is also less agreement that there are choices for how to prove who they are online
- Almost a quarter of those who have used government services state that they have had some kind of personal information leaked, hacked or used without permission

Concluding Thoughts…

GOVERNMENT

- Around half of people using government services trust the government to keep personal information safe. This is in line with the DINZ study done earlier this year
- There is also agreement that the government could be doing more to protect personal information online, although this is skewed more to those who don't trust the government saying this – we do also have citizens who do trust the government stating that more could be done
- The government has an opportunity to further instil trust and provide clarity on what it is doing to keep personal information safe

Concluding Thoughts…

REALME • Strong awareness of RealMe sitting at 80%, and over half of those who have used government services have used RealMe in the past 12 months. There is a correlation between age and awareness/usage; the younger you are the more likely you are to be aware and have used

- Good agreement that RealMe provided the service they were after. People are open to using RealMe outside of government services to some extent (62% agree)

ACTING ON BEHALF OF OTHERS

- Just over half of those who have accessed government services in the past 12 months have had to act on someone's behalf at some stage. More polarised responses with

regards to ease of acting on someone's behalf. Generally issues stem from either getting in contact with someone or establishing and proving access

A big

THANK YOU

for letting us

Yabble

Document 5

DIA: Project Services

Which government service or services have you used in the past 12 months?	What do you believe the government should be doing to protect your personal information online?	What did you find most difficult about the experience?	Gender	Ethnicity	Region	Household	Age group
Ird		Sending in information by attachment or getting a jp to sign documents	9(2)(a)		Auckland	Younger family	35-44
WINZ for community service card application WINZ for childcare subsidy assistance Studylink			9(2)(a)		Manawatu-Wanganui	Younger family	25-34
IRD, WINZ	not sure		9(2)(a)		Northland	Older family	35-44
Ird			9(2)(a)		Auckland	Older family	25-34
Land transport	Photo identification or some form of proof that only you would know		9(2)(a)		Auckland	Younger family	35-44
IRD	That it doesn't get hacked and your private info is kept that way.	Providing info and then having to repeat it a few	9(2)(a)		Hawke's Bay	Older family	45-54
Msd	Secured	What is real not spam	9(2)(a)		Christchurch	Older couple / Single	65-74
ACC	Contact us through email	Not difficult	9(2)(a)		West Coast	Older family	55-64
Work and Income IRD			9(2)(a)		Christchurch	Younger family	35-44
WINZ, IRD,	Making sure scammers and virus cannot access your information to steal your identity.		9(2)(a)		Auckland	Older family	45-54
IRD, Passport		n/a	9(2)(a)		Wellington	Older couple / Single	45-54
Ltsa		Sometimes didn't access online page correctly	9(2)(a)		Waikato	Younger family	35-44
Register new trailer	Make sure it's secure		9(2)(a)		Tasman	Older family	55-64
Health service, surgery.	Everything. Need to be reassured private medical information remains just that. Private.		9(2)(a)		Auckland	Younger family	45-54
Winz		n/a	9(2)(a)		Auckland	Older family	45-54
reg car	they should allready be doing it,		9(2)(a)		Bay Of Plenty	Older family	65-74
Internal affairs NZTA	Not sharing personal details with other agencies		9(2)(a)		Auckland	Older family	55-64
IRD, ACC, Tenancy services, work and Income			9(2)(a)		Auckland	Younger couple / Single	25-34

ird ms		better than ringing do it online faster	9(2)(a)		Bay Of Plenty	Younger family	25-34
ird		nothing	9(2)(a)		Manawatu-Wanganui	Older couple / Single	55-64
Work and Income		This was so that my 9(2)(a) could access medical equipment after 9(2)(a) surgery. 9(2)(a) was9(2)(a and able to sign for 9(2)(a) own surgery yet 9(2)(a) was unsure of 9(2)(a) rights and what help was available. The difficult part was extra support (making sure 9(2)(a) knew what 9(2)(a) was signing) availability (trying to make contact after school hours so that 9(2)(a) could verify/agree).	9(2)(a)		Auckland	Older family	35-44
Ird	Not sure	Nothing	9(2)(a)		Auckland	Younger family	25-34
IRD, Lotteries	Constantly updating legislation to reflect modern changes in how we as citizens operate online	remembering log in information that is not personal	9(2)(a)		Bay Of Plenty	Younger family	35-44
Inland Revenue Studylink ACC	Have multiple steps to get into the accounts		9(2)(a)		Auckland	Younger couple / Single	18-24
AT, to register a new car and sale of old							
car			9(2)(a)		Auckland	Younger family	35-44

Studylink	Introduce more extensive laws regulating what private companies can do with our personal information online		9(2)(a)		Wellington	Younger couple / Single	18-24
Inland Revenue			9(2)(a)		Auckland	Younger couple / Single	25-34
IRD	Better training for staff	The time taken and the lack of choices, and the inability to contact by phone	9(2)(a)		Southland	Older family	55-64
ird kiwisaver	keeping us informed what detail are held and current	imput infomation	9(2)(a)		Auckland	Older family	45-54
Registering a Vehicle	Have all protections in place so it doesn't fall into the wrong hands or get hacked.	The pages of information to read and the complicated system, rules and regulations are a nightmare to navigate through.	9(2)(a)		Hawke's Bay	Older couple / Single	55-64
nzta, hamilton council	making it more secure and asking about it once	asking for too many questions before giving answer	9(2)(a)		Waikato	Younger family	35-44
Tax vehicles		Filling in the forms	9(2)(a)		Manawatu-Wanganui	Older family	75+
Customs/immigration	Setting a NZ standard for companies to adhere to.	It was easy	9(2)(a)		Auckland	Older couple / Single	35-44
winz, ird, ministry of transport	Be more proactive, our personal info is sensitive and should be treated carefully and with respect and privacy	Dealing with IRD. I felt that I had no respect shown for my privacy	9(2)(a)		Hawke's Bay	Older couple / Single	65-74
WINZ	not sure sure, I would want to know anything I put online is viewed only by the intended person, agency and myself.		9(2)(a)		Auckland	Older family	65-74
Real me		Gaining access to services without having the right I. D	9(2)(a)		Auckland	Older family	35-44
Car registration		No issues	9(2)(a)		Auckland	Younger family	45-54
Department of Internal Affairs		Providing ID	9(2)(a)		Christchurch	Older family	65-74
Hospital	Better info		9(2)(a)		Bay Of Plenty	Younger couple / Single	25-34
nzpost & going to use ird & mymsd & real1	well better than they did for the treasury budget incident as if that is easy to get to what else is so need to know my information is safe		9(2)(a)		Auckland	Older family	25-34
Acc, Land transport		Nothing	9(2)(a)		Manawatu-Wanganui	Older family	35-44
Teaching Council	Ensuring any personnel who access sensitive information have adequate training.		9(2)(a)		Waikato	Younger family	25-34

Car registration	Send verification via txt with code or send via verification via email	people not knowing enough information about what you are asking about	9(2)(a)		Manawatu-Wanganui	Older family	35-44
renewed registration for a vehicle					Waikato	Older family	45-54
Car registration.	Taking steps to prevent identity fraud.	Setting up and forgetting passwords can make the process incredibly frustrating	9(2)(a)		Taranaki	Older couple / Single	25-34
IRD					Auckland	Older family	45-54
Winz Oranga tamariki	ensuring there is no leakage of anyones personal information to any party that it is not the intended recipient	Remembering my	9(2)(a)		Christchurch	Older family	45-54
IRD					Waikato	Older family	55-64
Tax	Secure it	Very slow	9(2)(a)		Manawatu-Wanganui	Older couple / Single	25-34
Winz	They not doing a good job				Auckland	Younger family	25-34
Teacher registration	I don't really know as I am not a technology expert.	Can't remember.	9(2)(a)		Auckland	Younger family	18-24
studylink					Wellington	Older family	55-64
Inland revenue	Keeping up to date with technology	No easy way to authorise another party to act.	9(2)(a)		Wellington	Older couple / Single	55-64
IRD	Make it more secure				Bay Of Plenty	Younger family	35-44
Council	Ensuring that no other person can access my information					Older couple / Younger couple / Single	
Acc	Security						
Department of social welfare		Some web sights were hard to follow	9(2)(a)		Christchurch	Single	25-34
Rego of vehicle, Ird		Was easy, all information needed was easily accessible				Younger couple / Single	
Vehicle registration, License renewal		Like IRD, its hard to get your child's details	9(2)(a)		Auckland	Younger family	25-34
IRD, DIA, NZ Vehicle	Ensure safe protection of data to keep it from being disclosed or hacked	Verification process required human interaction				Younger couple / Single	
DIA, IRD		Nothing	9(2)(a)		Waikato	Younger family	45-54
Vehicle registration	Everything they can	Proving my identity	9(2)(a)		Wellington	Younger couple / Single	25-34
car rego ird					Bay Of Plenty	Younger family	35-44
IRD	Have better way to differentiate people with similar names etc.	Professional people with not proper knowledge				Younger couple / Single	
IRD, immigration,	Better security	Paperwork	9(2)(a)		Auckland, West Coast		25-34
DHB	Only have network sharing if it is the resonable profile verification		9(2)(a)		Auckland	Older family	55-64
Ird	Have a better identification set in place	Navigation	9(2)(a)		Auckland	Younger couple / Single	25-34
New Zealand immigration			9(2)(a)		Waikato	Younger couple / Single	18-24
IRD			9(2)(a)		Christchurch	Younger couple / Single	35-44
IRD	Not too sure		9(2)(a)		Auckland	Younger couple / Single	35-44

Citizen	Strong firewall against		9(2)(a)		Auckland	Older couple / Single	45-54
Car registration			9(2)(a)		Manawatu-Wanganui	Older family	55-64
Ird	N/A	Na	9(2)(a)		Waikato	Younger family	35-44
NZTA, Winz, District health board, tax dpt,	Not sure, encryption of info, checking/verification methods, secure websites, for speakers of other languages having info in their language to communicate that their personal info is secure,	Not enough info on website, wasn't that obvious on the site, of contact details if you had problems interacting with the website (it was IRD). Esp. finding an 0800 phone no. to contact for personal help. It wasn't even included in the letter sent to the person, directing them to submit their personal info into the IRD website. Very frustrating. I did find it eventually, but for someone with low computer skills or literacy skills (reading), would have been very difficult. That contact phone no. should be on every webpage of the website and on every letter sent to people...for ALL government departments and services.	9(2)(a)		Otago	Older couple / Single	55-64
Driving licence, IRD number request	Protecting sensitive data from hacks. Identifying and securing weak points in data shared between departments	Proving their identity - lack of id verification docs	9(2)(a)		Auckland	Younger family	45-54
nzta	dont know		9(2)(a)		Christchurch	Older couple / Single	55-64
ACC, IRD, immigration			9(2)(a)		Auckland	Younger couple / Single	18-24
Ird	Secured website when logging in		9(2)(a)		Auckland	Younger couple / Single	25-34
NZ transport agency			9(2)(a)		Manawatu-Wanganui	Younger family	35-44
nz			9(2)(a)		Wellington	Older couple / Single	65-74
Work and income		Nothing	9(2)(a)		Manawatu-Wanganui	Younger family	25-34

Work and income	Have files that are family related to be blocked by other family members that work in the area	Itâ€™s wasnt secure enough	9(2)(a)		Auckland	Younger family	25-34
IRD	Secure storage of all data		9(2)(a)		Auckland	Older family	45-54
car registration			9(2)(a)		Christchurch	Younger couple / Single	25-34
Ird	Ensuring access is fully restricted to only the service being accessed.	Getting the authorisation	9(2)(a)		Manawatu-Wanganui	Older couple / Single	65-74
internal affairs	better security system, anything away from Hauwei		9(2)(a)		Auckland	Younger family	35-44
Internal Affairs	not share my info with a third party		9(2)(a)		Auckland	Older family	55-64
INZ, IRD			9(2)(a)		Auckland	Younger couple / Single	25-34
renewing driver's license IRD tax return	Stronger security for software and prevent leaks.		9(2)(a)		Auckland	Older family	25-34
Tax return	2 factor authentication		9(2)(a)		Auckland	Younger family	25-34
NZTA, IRD, Department of Building/Housing	Ensuring big tech companies (FB, Google etc) are held accountable for hacks/data breaches. Legislating what information can be stored and how it can be used.		9(2)(a)		Auckland	Younger couple / Single	25-34
Ird, enrolling to vote			9(2)(a)		Auckland	Younger couple / Single	25-34
ACC			9(2)(a)		Auckland	Older family	35-44
auckland hospitals	definetly	none as i know	9(2)(a)		Auckland	Younger family	25-34
Bond application	Not sure		9(2)(a)		Christchurch	Younger couple / Single	18-24
NZTA IRD	As much as possible	People understanding why they cant do it themselves	9(2)(a)		Auckland	Older couple / Single	35-44

Providing information for accident cover through ACC			9(2)(a)		Auckland	Younger couple / Single	25-34
Getting a new driver's license after original was stolen		Enormous amounts of paperwork and Dr visits and WINZ appointments. Very time consuming and the process took months.	9(2)(a)		Auckland	Younger family	35-44
Ird		Not difficult	9(2)(a)		Bay Of Plenty	Older couple / Single	55-64
ACC	Always to check ids	My9(2)(a) is of hard hearing telephone enquiries are most difficult and explaining 9(2)(a) problem to services can be stressful	9(2)(a)		Auckland	Older family	65-74
Renew passport	I am not sure but protection needs to be better		9(2)(a)		Auckland	Older family	45-54
ird	better security		9(2)(a)		Christchurch	Older couple / Single	45-54
IRD;	Investing in high tech security measures.	Getting access as that person.	9(2)(a)		Auckland	Older family	65-74
IRD			9(2)(a)		Wellington	Older couple / Single	75+
Change of car ownership when I bought a second hand	Use of an app or text code to confirm you are accessing a govt page and that it is actually you.	Nothing	9(2)(a)		Christchurch	Younger family	35-44
NZTA, IRD	2 factor logins on all websites. Verification if signed in from devices, or warnings		9(2)(a)		Christchurch	Younger family	35-44
Motor vehicle change of ownership		Remembering my login and password	9(2)(a)		Wellington	Older couple / Single	55-64
MyIR, NZTA change of address and	They need to better plan for risks and resource their network security teams properly to support the movement to					Younger couple /	
IRD	I am not knowledgeable with internet security so I cant suggest what they should do but I know the end result should be to feel confident that my information is safe with them	Going around in circles with the software and trying very hard to understand the processes ut not being able to work it out. Real me was especially difficult and incredible frustrating	9(2)(a)		Auckland	Older family	55-64
rid	better security, more staff, better technology		9(2)(a)		Auckland	Older family	65-74

Nzta applied for full licence		My 9(2)(a) has cerebral palsy with speech difficulty but is over 16 but the agency wouldn't let me speak on 9(2)(a) behalf. They also couldn't understand 9(2)(a) on the phone which made things impossible	9(2)(a)		Hawke's Bay	Younger family	35-44
RealMe			9(2)(a)		Christchurch	Younger family	35-44
internal affairs	limited access by people		9(2)(a)		Auckland	Younger couple / Single	35-44
passport agency			9(2)(a)		Tasman	Older couple / Single	45-54
NZTA			9(2)(a)		Wellington	Older couple / Single	55-64
Inland Revenue Dept	just make sure that it is keep secure		9(2)(a)		Christchurch	Older couple / Single	55-64
Inland revenue	Keep it secur		9(2)(a)		Bay Of Plenty	Older family	35-44
MSD		.	9(2)(a)		Waikato	Younger family	45-54
ACC, Car Registration	End-to-end encryption, 2FA enabled, encrypted databases	Often these services are poorly organised	9(2)(a)		Auckland	Younger couple / Single	25-34
Ird	Presently whatever information any	Nil	9(2)(a)		Auckland	Younger family	35-44
Vehicle registration, probably others but cant recall	individual government agency holds about me, is for the express purpose of that agency's need; I believe most NZers think there is a single information repository run by Govt which holds all the private information about NZers and people living in or visiting NZ. Provided each agency only accesses the particular information that it needs to conduct it's business with/for/on behalf of specific individuals, then that database should be created and maintained. Probably as a joint service between IRD, MSD, Justice/Corrections, MBIE, DIA, Health/DHBs ACC, HousingNZ etc (being the largest groups in the public service and state sector)	Being able to prove I held authority to act on behalf - required to provide multiple copies of that verification to the same agency/organisation/individual	9(2)(a)		Northland	Younger couple / Single	35-44

ACC Work and income Ird		Providing copies of documents	9(2)(a)		Christchurch	Younger couple / Single	25-34
Vehicle registration		Working through the company's web access management	9(2)(a)		Canterbury	Older couple / Single	45-54
IRD	GREATER INTERNAL CONTROLS	Getting some one to answer the phone	9(2)(a)		Wellington	Older couple / Single	65-74
Work and income		Nothing	9(2)(a)		Bay Of Plenty	Younger family	25-34
Car registration		the waiting	9(2)(a)		Canterbury	Older couple / Single	75+
ACC, IRD,	Ministers shouldn't have the ability to be able to see data about an individual and disclose	Establishing the right to access the	9(2)(a)		Canterbury	Older couple / Single	45-54
Vehicle registration			9(2)(a)		Wellington	Older couple / Single	65-74
Study link ACC	Secondary identification		9(2)(a)		Christchurch	Younger couple / Single	18-24
IRD , CAR LICENCE, NZ POST, WINZ	secure systems and procedures		9(2)(a)		Auckland	Older couple / Single	65-74
ACC						Younger couple /	
realme	laws about sharing personal information between agencies	proving my identity	9(2)(a)		Auckland	Younger couple / Single	35-44
Immigration			9(2)(a)		Canterbury	Younger family	35-44
Ird,work and income	not sure	not sure	9(2)(a)		Christchurch	Younger family	35-44
Ird	Not give your info to others or allow access to.		9(2)(a)		Auckland	Older family	55-64
Registration for car, student loan	To ensure things arent hacked, ie money taken from accounts		9(2)(a)		Otago	Older family	18-24
transport		nothing	9(2)(a)		Christchurch	Younger family	45-54

Motor vehicle registration	Ensuring that my personal details can not be hacked	Having to fill out forms and then being told that the EPoA trumps everything else	9(2)(a)		Bay Of Plenty	Older couple / Single	55-64
NZTA	Stronger firewalls on government websites	Remembering the log in credentials	9(2)(a)		Bay Of Plenty	Younger couple / Single	25-34
Ird	Not sure		9(2)(a)		Christchurch	Older couple / Single	55-64
Rent rebate from Council, Community Services Card renewal		tedious.	9(2)(a)		Otago	Younger couple / Single	45-54
Auckland Transport			9(2)(a)		Auckland	Older couple / Single	45-54
Winz	Protect it at all costs itâ€™s personal information they wouldnâ€™t like their details accessible for anyone so we should all be treated the same way as the Government we after all pay their salaries		9(2)(a)		Gisborne	Older family	45-54
Inland Revenue NZTA		Use Real Me to access IR for my business ... can't figure it out for my personal taxes though. Trying to call IR (even as I type!), got an automated callback (great!), but then advised computer system is down and it hung up on me. Guess I go to the back of the queue again ...?! (not great!)	9(2)(a)		Auckland	Younger family	45-54
Passport	Unsure	N/a	9(2)(a)		Auckland	Younger family	35-44
NZTA		providing permission from the child for me to act on their behalf	9(2)(a)		Waikato	Older family	45-54
ird		Wording of the question and where to find the answers, also having to hold on the phone for hours, only to be told its done on line	9(2)(a)		Bay Of Plenty	Older family	45-54
Vtnz	Better security		9(2)(a)		Waikato	Younger couple / Single	35-44
IRD, ACC, do Hospitals count?		Canâ€™t think of anything	9(2)(a)		Wellington	Older couple / Single	55-64

acc	Information sharing is both a necessity and a problem. Information needs to be shared if it is to help the individual or the family (eg health services & ACC). I would like to know who potentially could access the data. This is not necessarily about limiting access to data its about making sure the right people have access to it and the people who don't need to know don't. So I believe the government should protect my personal information on a need to know basis and that this is best achieved by being transparent about who has access to my data and giving me the opportunity to choose who can access it and explaining to me, truthfully, any issues that may arise (positive and negative) from those choices.	1) Proving that I had the right to access the data & 2) Remembering Usernames and passwords to access data particularly where passwords are regularly required to be updated.	9(2)(a)		Waikato	Older couple / Single	65-74
		Learning the process and getting				Younger couple /	
A cc	Make it clear what they are doing with your private information and who will access ot	Remebering all the logins and passwords	9(2)(a)		Waikato	Older family	55-64
nzta driver licensing, aa, post office	everything they possibly can	they dont give out any information until they hear from the person in question for authority. very difficult when you are an employer asking about the employees training	9(2)(a)		Otago	Younger family	25-34
Car registration	Protect it from misuse	Too much info asked	9(2)(a)		Auckland	Younger couple / Single	35-44
MOT			9(2)(a)		Tasman	Older family	65-74
Winz	Unsure	Inability to get photo ID for 15-16yr olds who don't get school id	9(2)(a)		Manawatu-Wanganui	Older family	35-44
IRD website	If RealMe is ever used outside of government departments the requirements and security needs to be top notch. As shown by Treasury this week, their IT security and practices are not top of practice	Verifying I was from a business with a valid cause wasn't as easy or at times didn't seem as difficult as I thought it should be	9(2)(a)		Wellington	Younger family	35-44
NZTA		Red tape Passwords	9(2)(a)		Auckland	Younger family	25-34
IRD		getting login details from clients	9(2)(a)		Waikato	Younger couple / Single	25-34

Companies Register	using Real Me does this	when you have to talk to someone	9(2)(a)		Wellington	Younger family	35-44
Ird,			9(2)(a)		Auckland	Younger couple / Single	45-54
Ird	More security checks	Wait time	9(2)(a)		Bay Of Plenty	Younger family	25-34
IRD, ACC,		Verifying the identification with Post shop.	9(2)(a)		Auckland	Older family	55-64
ACC - Paying levies, NZTA - registration, moving house, IRD - Filing returns, moving house, refunds, WINZ - apply for a benefit	I'm worried about my details not being anonymised when doing for data mining. I'm not convinced that the information practices are being followed that protect the information of users. I would want more assurances of this.	Trying to get authority on the account was quite tricky	9(2)(a)		Wellington	Younger couple / Single	25-34
registered a car			9(2)(a)		Auckland	Older couple / Single	45-54
Car registration, IRD, passport renewal		Set up a RealMe ID for my 9(2)(a) with a token from 9(2)(a) Android phone, but we replaced the phone and 9(2)(a) couldn't log in any more, so was trapped. Had to call a helpline to get the 2FA taken off 9(2)(a) account. Was pretty frustrating.	9(2)(a)		Auckland	Older family	55-64
Will	Make access with passwords easier.		9(2)(a)		Otago	Younger couple / Single	25-34
Internal affairs, inland Revenue		Nothing specially	9(2)(a)		Northland	Older couple / Single	55-64
ACC			9(2)(a)		Waikato	Younger couple / Single	18-24
Road tax registration motor vehicle Diesel			9(2)(a)		Taranaki	Older family	65-74
Identity (passport) IRD	making sure it is obvious it is secure	nothing	9(2)(a)		Christchurch	Younger family	45-54
Car registration	No idea sorry.	Getting hold of someone to talk to on the phone.	9(2)(a)		Bay Of Plenty	Older family	45-54
NZTA	Never sell to any other party. Remind us to keep it secure.	Overseas death of my 9(2)(a). Had to get English certified copies of 9(2)(a) death certificate to close up bank accounts here.	9(2)(a)		Christchurch	Older family	25-34

						Younger couple /	
Tax refund	Not sure but it just feels like my info is not safe. Also places like WINZ should not have to know every single tiny detail about what you're doing and where you are going.		9(2)(a)		Auckland	Younger couple / Single	18-24
Drivers License	Not sure		9(2)(a)		Auckland	Older couple / Single	75+
IRD, WINZ		Trying to find a way out when you hit a wrong button, or the answer was not sufficient for the question.... to then try contacting a HUMAN was impossible. I gave up on three or four separate occasions. NO ONE at a government department answers the bloody phones any more - Where are all the staff?	9(2)(a)		Auckland	Older couple / Single	55-64
health	safe	your not agnowlege	9(2)(a)		Hawke's Bay	Older couple / Single	65-74
hospital			9(2)(a)		Auckland	Older couple / Single	65-74
Applying for a passport		Figuring out what information i was actually required to provide, before trying to do whatever it was i was trying to do	9(2)(a)		Canterbury	Younger family	25-34
NZTA, RealMe	Everything it can	Nothing really	9(2)(a)		Bay Of Plenty	Younger couple / Single	45-54
IRD			9(2)(a)		Waikato	Younger couple / Single	25-34
ACC	Just protect it and not pass on but then they cant even protect their budget information	answering questions and also just making contact over the phone without having to wait 10 minutes while they play disgusting music	9(2)(a)		Canterbury	Older family	55-64
ACC, IRD, MSD	Not share info unless agreed	Ensuring other people as office holders were involved	9(2)(a)		Auckland	Older couple / Single	75+
RealMe IRD MOT		Although I advised the IRD three times that my partner had died they continued to make mistakes with 9(2)(a details and their merge letters were obviously not checked before printing and sending as they continued to make errors in dealing with the closing of 9(2)(a Tax accounts, donation receipts etc.	9(2)(a)		Auckland	Older family	45-54

ird		Which experience are we talking about here? For my tax returns there were no difficulties. Finding the time to do them was the greatest hurdle.	9(2)(a)		Christchurch	Older couple / Single	45-54
Nice	Donâ€™t share it with permission		9(2)(a)		Auckland	Older family	45-54
Tax Department	There appears to be some hacking of Govt info so they may need stronger securuty		9(2)(a)		Bay Of Plenty	Older couple / Single	55-64
ACC		Nothing particularly.	9(2)(a)		Auckland	Younger family	45-54
NZTA	Add more security and firewalls	More questions	9(2)(a)		Auckland	Younger couple / Single	25-34
Register a	Greater		9(2)(a)		Wellington	Older couple / Single	55-64
Updating voting information			9(2)(a)		Auckland	Younger couple / Single	25-34
ACC			9(2)(a)		Auckland	Younger couple / Single	35-44
Regsitration, Road users & passport		Getting help when required	9(2)(a)		Waikato	Older couple / Single	55-64
rego renewel	never diclouse it		9(2)(a)		Bay Of Plenty	Older couple / Single	45-54
Dept of Internal Affairs						Older couple /	
Tax return and registered car			9(2)(a)		Christchurch	Younger couple / Single	18-24
Border control (customs, immigration, MPI)		Proving that the other person wants me to act on their behalf, when that other person does not speak English, and does not live in the same area as me, so cannot come to the phone while I am trying to do the business.	9(2)(a)		Bay Of Plenty	Older couple / Single	55-64
IRD, Birth Regestration, Best Start, Passport for Son		Nothing	9(2)(a)		Auckland	Younger family	35-44
Ird	Whatever is necessary to		9(2)(a)		Auckland	Older couple / Single	65-74

ird			9(2)(a)		Wellington	Older couple / Single	65-74
Ird		I find everything is usually pretty straightforward, itâ€™s usually the lack of communication	9(2)(a)		Wellington	Younger family	25-34
Transport	making sure nobody else has access	Proving my identity	9(2)(a)		Northland	Older couple / Single	75+
NZ Transport, IRD			9(2)(a)		Nelson	Older couple / Single	25-34
NZTA			9(2)(a)		Otago	Younger couple / Single	35-44
Companies registry, Passport.	They need to be punishing local and international platform providers (eg Facebook) if our data is misused. The outputs of the upcoming new privacy act need to be properly communicated so people understand their rights and ownership of their own data, and the right to access it and move it within organisations. They need to be investing more in awareness of what people can do to stay secure online.	Not sure I have an answer for this.	9(2)(a)		Auckland	Older family	45-54
nzta	I dont want to use it as I feel my info is not safe and then I don't get the paper reminders as they expect you to check the system and do things through it	making sure had correct paperwork	9(2)(a)		Auckland	Younger family	35-44
IRD			9(2)(a)		Auckland	Older family	55-64
Inland Revenue, car registration.			9(2)(a)		Canterbury	Younger family	25-34
car registration	Using two-factor authentication		9(2)(a)		Waikato	Older couple / Single	45-54
Ird			9(2)(a)		Northland	Older couple / Single	65-74
govt nz - passport	Personal details needed to be secure and confidential, not able to be hacked		9(2)(a)		Otago	Older couple / Single	45-54
LTSA, registing a car	I dont want any 3rd party to get my information		9(2)(a)		Hawke's Bay	Older couple / Single	55-64

ACC		Having to remember to take my paperwork to the bank	9(2)(a)		Christchurch	Older family	55-64
ACC WINZ IRD	Unsure	The lack of Clear spoken English on 0800 numbers. The lack of offices to attend in our region. Not certain of entitlements	9(2)(a)		Bay Of Plenty	Younger family	45-54
Registering a vehicle, IRD (My IR), paying a speeding ticket, applying for a Trademark	constantly be updating security systems and informing us as they do so	Just lots of information to fill out and read	9(2)(a)		Auckland	Younger couple / Single	25-34
IRD, Passports	Invest in better online security	Cumbersome process	9(2)(a)		Auckland	Younger family	35-44
IRD	better encryption, tighter personal information protection law	time to prepare the required documents	9(2)(a)		Auckland	Younger family	45-54
Inland revenue, RealMe	Making sure that the data that is held is secure from	Getting through the wait times, having the person actually understand the issue	9(2)(a)		Auckland	Younger couple / Single	18-24
NZ Passport			9(2)(a)		Hawke's Bay	Older couple / Single	45-54
Nzta	Make sure personal information isn't shared by a 3rd party	A oong process requesting a passport for a child	9(2)(a)		Bay Of Plenty	Younger family	45-54
ACC	As much as possible		9(2)(a)		Auckland	Older couple / Single	35-44
Electrical Workers site			9(2)(a)		West Coast	Older couple / Single	65-74
NZTA RUC, RealMe,		Websites are often confusing trying to find the information you need or difficult to upload to	9(2)(a)		Wellington	Older family	55-64
IRD Car			9(2)(a)		Christchurch	Older couple / Single	65-74
IRD tax return			9(2)(a)		Auckland	Younger couple / Single	18-24
Car registration	Ensure info supplied is not able to be hacked and not shared with any other non-govt agency.	Didn't experience difficulty	9(2)(a)		Christchurch	Older couple / Single	45-54
NZQA	Stronger security. Minimise risk of leaks (such as what has happened in the UK and Australia in recent years).		9(2)(a)		Auckland	Older couple / Single	45-54

NZTA, IRD, Ministry of Health		The online systems dont always make it easy to understand what they want or I provide an email address and they keep saying its not valid??	9(2)(a)		Bay Of Plenty	Older family	55-64
Tax return, car registration			9(2)(a)		Auckland	Younger couple / Single	45-54
NZTA			9(2)(a)		Auckland	Older couple / Single	55-64
RealMe, IRD, BDM website			9(2)(a)		Waikato	Younger couple / Single	25-34
Internal			9(2)(a)		Hawke's Bay	Older couple / Single	65-74
Passport renewal		Proving I had POA	9(2)(a)		Auckland	Younger family	35-44
Work and income, LTSA, IRD	Ensuring that personal information is encrypted, secure and not accessible in anyway apart from where information needs to be shared.		9(2)(a)		Auckland	Older family	35-44
WINZ, Car reg			9(2)(a)		West Coast	Older family	45-54
Register a vehicle, work and income family tax credits, work and income childcare subsidies		process to prove identity	9(2)(a)		Northland	Younger family	35-44
Rego			9(2)(a)		Otago	Younger family	45-54
ACC Passport	More Online Security		9(2)(a)		Auckland	Younger family	55-64
IRD	There should be more Encryption method used for personal information over the internet		9(2)(a)		Otago	Older couple / Single	55-64
Companies Office, passports, car rego			9(2)(a)		Christchurch	Younger family	45-54
Inland revenue	More secure local storage		9(2)(a)		Waikato	Younger family	35-44
Ministry of Social Development		Constantly explaining my role in another person's life and having agencies requiring proof, double proof and then checking up on me.	9(2)(a)		Bay Of Plenty	Older couple / Single	55-64

Nzta			9(2)(a)		Auckland	Younger couple / Single	25-34
A.A.			9(2)(a)		Auckland	Older family	25-34
EWRB	Educating people	Understanding government-speak	9(2)(a)		Auckland	Older family	55-64
MSD			9(2)(a)		Auckland	Older couple / Single	75+
VTNZ	Unsure how spam callers are getting my number and know my name etc when I dont put my info on any untrusted		9(2)(a)		Northland	Older couple / Single	18-24
Acc, Wtnz.	make sure hackers cannot get into the system.		9(2)(a)		Auckland	Older family	65-74
	keeping up to date with the ways and means by which cyber criminals steal this				Manawatu-	Younger couple /	
winz and ird	Do more to prevent hacking and have a better phone service.	The fact that I never received return calls or replies to a letter.	9(2)(a)		Otago	Older couple / Single	65-74
Registration, BDM Certificates	more that it is now but not sure what, hackers are always getting smarter		9(2)(a)		Waikato	Older family	45-54
ird		can't remember	9(2)(a)		Waikato	Younger couple / Single	35-44
Registered		Nothin	9(2)(a)		Auckland	Younger family	25-34
WINZ	?		9(2)(a)		Auckland	Older couple / Single	35-44
Vehicle registration	Not sharing data with other people, cyber security. The budget was hacked today!!	RealMe online was very unfriendly	9(2)(a)		Auckland	Younger family	45-54
Internal Affairs	Request a person's permission before sharing info about them to others	The age of children being classed as an adult is different for different organisations/services so it makes it hard to know as a parent when they have to act for themselves.	9(2)(a)		Auckland	Older family	45-54
NZTA	secure my information, make sure that no one can have access to it apart from government use		9(2)(a)		Christchurch	Older family	18-24

IRD	Just better security layers. The day has come when it is too easy to steal identity.	Remembering user names and passwords	9(2)(a)		Northland	Older family	45-54
IRD	Ensure security measures are always in place online	Creating a long enough password to be secure	9(2)(a)		Wellington	Older family	45-54
Applying for a passport		Nothing	9(2)(a)		Wellington	Younger family	25-34
department of internal affairs			9(2)(a)		Auckland	Older family	55-64
Acc	Ensure hackers can't access my personal information	Getting the person on the other side to agree to assist	9(2)(a)		Auckland	Older family	65-74
Applied for a new passport			9(2)(a)		Auckland	Older couple / Single	65-74
Elector registration, Car change of ownership	second level verification, SMS code, etc.		9(2)(a)		Waikato	Younger couple / Single	35-44
Ird. Nzta.	Secure database such as	Na	9(2)(a)		Canterbury	Younger couple / Single	25-34
ird, nzta, msd	not sure	process	9(2)(a)		Wellington	Younger family	25-34
NZTA	Ensure my information cant be hacked or stolen		9(2)(a)		Taranaki	Older couple / Single	45-54
Internal Affairs for a passport renewal.	There are always going to be hackers, private corporate and state sponsored, who will attack with the intention of breaking into any system. Every organization needs to be super careful of all third party info it holds. I, at least, trust the NZ Government not to sell personal information to other parties like Facebook does.		9(2)(a)		Auckland	Older couple / Single	65-74
winz			9(2)(a)		Taranaki	Older couple / Single	65-74
Work and Income, Inland Revenue,ACC	I am not exactly sure, but those that are caught using the information when they shouldn't should face large financial loss and prison time.		9(2)(a)		Auckland	Older family	55-64
IRD, Transport Agency	By using RealMe or similar		9(2)(a)		Canterbury	Older couple / Single	75+
Department of Internal Affairs			9(2)(a)		Christchurch	Older family	55-64

myGov, WINZ, transprt, myhealth	Hiring ex-hackers/contractors to look for flaws in the security systems.		9(2)(a)		Auckland	Younger couple / Single	25-34
IRD		It's difficult to get put through to the right person	9(2)(a)		Auckland	Younger family	35-44
MSD	ensuring that only yourself and specific departments can access.		9(2)(a)		Christchurch	Older couple / Single	65-74
Work and Income, Internal Affairs		Verifying Identity and accessing the right department	9(2)(a)		Auckland	Older couple / Single	65-74
hospital, rego		getting the authority to speak on behalf of	9(2)(a)		Waikato	Older couple / Single	55-64
Work and Income		Waiting on phone	9(2)(a)		Auckland	Older couple / Single	65-74
IRD		Nothing I just had to prove I was the 9(2)(a)	9(2)(a)		Auckland	Younger family	35-44
IRD		Bearing in mind this was some time ago (approx 25 years) I found the interface slightly threatening toward all parties.	9(2)(a)		Marlborough	Older couple / Single	65-74
IRD ACC	Through appropriate security systems		9(2)(a)		Auckland	Older couple / Single	55-64
LINZ, MBIE, Companies Office	Unsure - I am not an expert in this area	Providing the necessary evidence to show that I was authorised by my 9(2)(a)	9(2)(a)		Auckland	Older family	45-54
Reregister the car Winz	have very limited acces to it	That they still had my details from a previous action I had taken	9(2)(a)		Christchurch	Older family	65-74
Winz, drivers licensing	Not sure		9(2)(a)		Auckland	Younger couple / Single	25-34
Ird		Time it took	9(2)(a)		Manawatu-Wanganui	Older family	45-54
IRD	Keeping secure so cannot be accessed by anybody not entitled to by law.		9(2)(a)		Auckland	Older family	65-74
IRD	being very careful storing and exporting any personal information	nothing	9(2)(a)		Marlborough	Older family	45-54

WINS. IRD	WINS interviews should be in private not open room	number of time being ask the same silly questions, and the person I was try to help also being asked, when they did not speek english	9(2)(a)		Canterbury	Older family	65-74
AA	To assure people their information online ar e safe and	Not at	9(2)(a)		Christchurch	Older family	45-54
IRD, ACC, MOH, MOT.		Not having the necessary paperwork to hand in an emergency	9(2)(a)		Canterbury	Older couple / Single	55-64
Internal affairs for new passport		Understanding government speak/terms.	9(2)(a)		Bay Of Plenty	Older family	55-64
winz			9(2)(a)		Canterbury	Older couple / Single	65-74
Inland Revenue AT Transport Toll		Not sure	9(2)(a)		Auckland	Younger family	18-24
ministry of transport			9(2)(a)		Southland	Older couple / Single	55-64
passport renewal, acc			9(2)(a)		Canterbury	Older couple / Single	65-74
Inland Revenue	To ensure only the right level of access is provided to the agency. And to ensure the information is stored securely.	To provide proof of relationship	9(2)(a)		Auckland	Younger family	35-44
NZTA			9(2)(a)		Auckland	Older couple / Single	65-74
My msd, ird		Privacy issues, and getting someone ro believe your purpose is genuine	9(2)(a)		Waikato	Older couple / Single	55-64
ACC, licencing car ; citizenship application , passport	Strong security in all platforms with one time authentication codes	The fact I could not act for a child when necessary	9(2)(a)		Manawatu-Wanganui	Older couple / Single	55-64
WOF, hospital, IRD	Have up to date security services and not share my info		9(2)(a)		Wellington	Older couple / Single	45-54
Itsa	protect info	nothing	9(2)(a)		Christchurch	Younger family	65-74
Ird, work and income, nz government,	?		9(2)(a)		Bay Of Plenty	Younger family	35-44

dont know vehicle registration probably	not sure just wmore		9(2)(a)		Christchurch	Younger couple / Single	25-34
	Make you change your password after a certain period of	.	9(2)(a)		Auckland	Older family	35-44
IRD	Not sure, online personal information should be the responsibility of the individual however there are so many companies trading personal information that this practice should be banned		9(2)(a)		Auckland	Older family	45-54
ACC, registered a car, visa update on	Making access to things like real me free, allowing info to be uploaded online						
IRD			9(2)(a)		Christchurch	Younger couple / Single	25-34
IRD, Local council, tolls	all agencies within government interchange information BUT at times without my knowledge. Any dept that interacts and takes information needs to have my OK before hand.		9(2)(a)		Bay Of Plenty	Older couple / Single	65-74
Passport, ird, driving	Strong	Nothing in	9(2)(a)		Bay Of Plenty	Younger family	35-44
Car registration and IRD			9(2)(a)		Christchurch	Younger family	35-44
ACC,IRD			9(2)(a)		Auckland	Older family	55-64
NZTA	Making sure its secure	Nothing	9(2)(a)		Auckland	Younger family	35-44
NZTA, ACC, Breast Screening Aotearoa	Everything in its power.	When to use RealMe rather than an alternative.	9(2)(a)		Auckland	Older couple / Single	45-54
NZTA, acc, IRD	transparency regarding data protection and how data is stored/protected	can't remember the specifics but I think it was trying to provide additional information. Definitely difficult with NZTA to do anything when you own a business vehicle!!!!	9(2)(a)		Auckland	Younger couple / Single	35-44
Ird	Na	Taking all the papers	9(2)(a)		Christchurch	Older couple / Single	45-54
RealMe			9(2)(a)		Auckland	Younger couple / Single	35-44

Car registration	Making sure the information is kept secure	Proving I was who I said	9(2)(a)		Auckland	Older couple / Single	65-74
IRD	Well they just got their budget hacked, so need to tighten things up I would say.	Nothing, it was easy.	9(2)(a)		Bay Of Plenty	Older couple / Single	45-54
birth registration, tax return	make sure it cant be accessed by unauthorised people	long forms, amount of information required, repetative questions	9(2)(a)		Southland	Younger family	25-34
IRD NZTA	Inform people of how they use personal information	Finding the documentation to verify identity	9(2)(a)		Bay Of Plenty	Younger family	25-34
ACC		The wait times on the phone	9(2)(a)		Auckland	Older family	45-54
IRD, WINZ	improve encription, reduce access by 3rd parties, stay ahead of hackers and disrupters		9(2)(a)		Auckland	Older couple / Single	65-74
Vechile registration	Protect how my data is used by other	The amount of detail	9(2)(a)		Wellington	Younger family	35-44
Tenancy Services, Work and Income, IRD		Some times it should be convenient to just scan and upload the documents, like Studylink uses Connect service	9(2)(a)		Wellington	Younger family	35-44
IRD, DIA			9(2)(a)		Wellington	Younger couple / Single	25-34
IRD	Providing more information about how our information is kept secure		9(2)(a)		Auckland	Younger couple / Single	18-24
Work and Income, Land Transport, Inland Revenue	make sure it is kept private for their use only	getting authority to act on behalf of the person, but that is not a bad thing	9(2)(a)		Tasman	Older family	65-74
Registering a car	Not sharing it		9(2)(a)		Southland	Younger family	18-24
Work and income	Ultra tight security		9(2)(a)		Auckland	Older family	55-64
acc,wof	don't give it out		9(2)(a)		Taranaki	Younger couple / Single	45-54
drivers licence	not sure		9(2)(a)		Hawke's Bay	Older couple / Single	65-74
NZPost	Not	The length of time to get a	9(2)(a)		Manawatu-Wanganui	Older couple / Single	45-54

Work and	Stop giving third		9(2)(a)	Auckland	Older family	45-54
Tax, ACC		Was ok, although a bit of red tape and for filling to go through	9(2)(a)	Otago	Younger couple / Single	45-54
IRD		Nothing.	9(2)(a)	Christchurch	Younger couple / Single	25-34
Car registration		nothing	9(2)(a)	Auckland	Older family	55-64
IRD	encouraging better security practices, and supporting people to verify their digital ID by making it straightforward and cheap/free to do so	proving it was okay to be doing it	9(2)(a)	Christchurch	Older family	55-64
		I was given authority but it never got documented so had to go through the				
Renewed Passport, ACC & Car Registration			9(2)(a)	Hawke's Bay	Older family	55-64
IRD, car registration		nothing	9(2)(a)	Bay Of Plenty	Younger family	35-44
Work and Income	Making sure that there online services are secure so that no one can hack other peoples personal information		9(2)(a)	Manawatu-Wanganui	Older couple / Single	45-54
ACC	More secure storage and access of information	Prooving who is was	9(2)(a)	Canterbury	Older family	55-64
ACC, IRD		N/A	9(2)(a)	Christchurch	Older family	45-54
ird		not sure	9(2)(a)	Otago	Younger couple / Single	25-34
registered a vehicle		having to prove who I was all the time	9(2)(a)	Wellington	Older couple / Single	55-64
ACC, WINZ,	Too many leaks from online	Nothing	9(2)(a)	Auckland	Younger family	25-34
new passport	ensure they have good cyber security in place	having to jump through too many hoops to get information	9(2)(a)	Auckland	Older family	45-54
Study link My Ird	Encrypting and making it impossible to share	The request for I'd or photo id for a child, if they have no passport it doesn't exist.	9(2)(a)	Christchurch	Older family	45-54

Acc	Have top line security		9(2)(a)		Auckland	Older family	65-74
Ltsa	Dont know	It was ok	9(2)(a)		Auckland	Younger family	35-44
ACC		proving I had authority to act on behalf of the person/organisation	9(2)(a)		Wellington	Younger family	25-34
IRD, Passport, ACC			9(2)(a)		Christchurch	Younger couple / Single	25-34
IRD	Promote password services like Lastpass		9(2)(a)		Auckland	Younger couple / Single	35-44
ACC, IRD		Just the time it took to wait on the phone.	9(2)(a)		Auckland	Younger couple / Single	25-34
IRD			9(2)(a)		Auckland	Younger family	35-44
Vehicle Licensing (NZTA)		Having all of the required verification information, often you don't know what you need until you are part way through the process	9(2)(a)		Auckland	Younger family	45-54
IRD NZTA	Ensure a consistent and secure identity across govt departments. Allow external parties eg Banks to use RealMe as a proof of identiy but not to divulge personal/govt data	Proving identity	9(2)(a)		Auckland	Older couple / Single	55-64
Application for community services card, register for parental leave		Having correct login details	9(2)(a)		Christchurch	Younger couple / Single	25-34
ACC			9(2)(a)		Auckland	Younger couple / Single	18-24
Studylink		Remembering all the different details especially when you don't use it often enough	9(2)(a)		Bay Of Plenty	Younger family	25-34
ACC	Privacy	Process to verify	9(2)(a)		Auckland	Younger family	35-44
ird		Using the correct password	9(2)(a)		Taranaki	Younger family	45-54
vehicle registration	Encrypt data, provide anti-hacking measures.	Dealing with snotty receptionists.	9(2)(a)		Otago	Older couple / Single	55-64

Inland Revenue			9(2)(a)		Hawke's Bay	Younger couple / Single	18-24
MSD / WINZ, The Transport Agency	We all have heard through the media stories of peoples personal info going to the wrong people [ACC], currently parts of the budget 2019 being leaked - what does that say about the Govt,'s security ?		9(2)(a)		Hawke's Bay	Older couple / Single	55-64
Car registration, filing company return, inland	Have the strongest security but don't make it too difficult for the end user. A credit card type of ID could be introduced.	Remembering password etc....	9(2)(a)		Hawke's Bay	Younger family	35-44
WINZ, Car Rego,	Not sure. At my age it becomes more difficult to remember passwords etc		9(2)(a)		Auckland	Older couple / Single	65-74
IRD	Not a tech guru myself, but as much as they possibly can.	Nothing comes to mind.	9(2)(a)		Bay Of Plenty	Older couple / Single	45-54
		Information often isn't clear. Not enough					
WINZ			9(2)(a)		Waikato	Older couple / Single	65-74
Passport	You dont know if its protected. You just have to trust it is		9(2)(a)		Auckland	Older couple / Single	55-64
WINZ	Make it so it is only accessible to those who need it.		9(2)(a)		Waikato	Younger family	45-54
Ministry of Social Development			9(2)(a)		Otago	Older couple / Single	65-74
IRD, NZTA, ACC		Verification of access	9(2)(a)		Tasman	Older couple / Single	55-64
MSD acc			9(2)(a)		Tasman	Older couple / Single	65-74
WINZ	Confirm with New Zealand post/banking correct person	Remembering other passwords	9(2)(a)		Wellington	Younger couple / Single	25-34
IRD		The forms you had to fill in	9(2)(a)		Manawatu-Wanganui	Younger family	45-54
ACC, Governmebnt Superannuation, Vehicle Licencing		Found it reasonably OK but I had been well briefed as to how to exercise the power of attorney.	9(2)(a)		Hawke's Bay	Older couple / Single	65-74

Registering		Nothing	9(2)(a)		Wellington	Younger couple / Single	25-34
m s d, transport, police i r d,	everything possable	officiouse little twats that know nothing but can cut you off	9(2)(a)		Northland	Older family	55-64
IRD		Figuring out that I needed to put a 0 in front of my IRD number online	9(2)(a)		Bay Of Plenty	Younger family	35-44
Internal	Stronger security software		9(2)(a)		Christchurch	Older couple / Single	45-54
IRD			9(2)(a)		Christchurch	Younger couple / Single	25-34
IRD, vehicle registration, passport renewal	Encryption of all		9(2)(a)		Auckland	Older couple / Single	45-54
IRD	Not sure	None	9(2)(a)		Auckland	Older family	18-24
NZTA	Not sure		9(2)(a)		Auckland	Older family	75+
Registering myths car.			9(2)(a)		Auckland	Older couple / Single	75+
IRD, Studylink		being expected to remember all of someone else's passwords...	9(2)(a)		Auckland	Older couple / Single	18-24
NZTA vehicle registration	Stronger and more frequent audits of security of departmental/agency systems, and require vetting of all staff who deal with my/your personal information.	The idiotic automated telephone systems that will not give an option to speak to a real person - any agency/department that has those systems generally has a very poor customer approach - it is certainly not worth calling it service - and a high level of its own importance - arrogance even.	9(2)(a)		Wellington	Older couple / Single	65-74
Ird			9(2)(a)		Wellington	Younger family	35-44
winz		wait time when on phone	9(2)(a)		Southland	Older family	45-54
ACC	Encryption		9(2)(a)		Christchurch	Older family	45-54
None			9(2)(a)		Canterbury	Younger couple / Single	25-34

Healthcare New Zealand			9(2)(a) 9(2)(a)		Otago	Older couple / Single	75+
Ministry for Social Development		I don't find it difficult at all	9(2)(a)		Bay Of Plenty	Older family	45-54
Ird	They should not share information between departments more checks	getting a person to speak to	9(2)(a)		Waikato Southland	Older couple / Single Younger family	55-64 35-44
ACC, NZTA, IRD	Requiring that tech companies store their NZ-sourced data locally. Add 2-factor authentication to RealMe	Trying to help 9(2)(a) with information on an issue that we both jointly liable, and not being able to solve a problem involving	9(2)(a)		Auckland	Younger family	25-34
ACC	Ensuring no-one can access it without legal and compelling reason	Not understanding the keywords (jargon)	9(2)(a)		Auckland	Older family	55-64
work & income	Security is a very important and delicate	Password in some domains is numeric, in others Alphanumeric	9(2)(a)		Auckland	Older couple / Single	55-64
IRD	business. I really donâ€™t know how any Introduce fingerprint technology and/or	them when they were incapacitated	9(2)(a)		Wellington	Older family	65-74
Passport Renewal and IRD	information stored online can be facial recognition to prevent unauthorised absolutely secure access to my data by others	Having to meet face to face for a process	9(2)(a)		Auckland	Older family	65-74
Accommodation Supplement. Passport office. Jobseekers Benefit	Make sure their servers are well protected Minimum two factor authentication from hackers.	that took mere	9(2)(a) 9(2)(a)		Auckland Auckland	Older couple / Younger family Single	35-44 65-74
	Ensure details are not emailed to the wrong recipients!						
IRD, passports, work and income,	Once we have confirmed our identity, allow sharing of this information.		9(2)(a)		Manawatu-Wanganui	Older couple / Single	65-74
Defence	Need to insure it can only be accessed by those with authority	Not knowing what information was required	9(2)(a)		Manawatu-Wanganui	Older family	55-64
ACC	Audit more big business	unknown	9(2)(a)		Wellington	Younger family	35-44
IRD			9(2)(a)		Manawatu-Wanganui	Older couple / Single	65-74
Ird		Disnt	9(2)(a)		Christchurch	Older couple / Single	45-54
Ird, and passport services			9(2)(a)		Waikato	Younger family	35-44
Renewing registration on a car			9(2)(a)		Auckland	Younger family	35-44
Immigration, Inland revenue and RealMe			9(2)(a)		Auckland	Younger couple / Single	25-34
Ird			9(2)(a)		Christchurch	Younger family	25-34

NZTA Drivers licensing and ACC	There needs to be more attention paid to online security but also to check that posted information is going to the right person. I received someone elses letter in the envelop with my letter.	You have to keep repeating information when you are transferred to someone else in department transfers	9(2)(a)		Auckland	Older family	45-54
Passport	Unsure	Often got conflicting information as to what I could or couldn't do from same organization, but different people	9(2)(a)		Otago	Older family	45-54
IRD		Proof of POA FOR ELDERLY RELATION	9(2)(a)		Auckland	Older couple / Single	55-64
ird working for family's dhb	better training for staff in customer verification	paper work	9(2)(a)		Northland	Older family	45-54
WINZ IRD LAND TRANSPORT AUTHORITY		Can't recall	9(2)(a)		Christchurch	Older couple / Single	65-74
Renew		Nothing	9(2)(a)		Bay Of Plenty	Younger family	35-44
car registrationâ€(	-	-	9(2)(a)		Manawatu-Wanganui	Younger couple / Single	18-24
Ministry of Transport - Car registration Internal Affairs - passport renewal			9(2)(a)		Canterbury	Younger family	25-34
Births deaths marriages. Acc			9(2)(a)		Christchurch	Younger family	25-34
2018 consensus	Making sure that a limited number of groups have access to the information,		9(2)(a)		Otago	Younger family	18-24
RealMe	Transparent data security		9(2)(a)		Auckland	Younger couple / Single	18-24
Ird	They can do things like sending code to mobile to enter online	To prove I am a authorized person .	9(2)(a)		Auckland	Younger family	45-54
Ird			9(2)(a)		Christchurch	Younger couple / Single	25-34
Work and Income			9(2)(a)		Auckland	Older couple / Single	75+
I think it was ACC			9(2)(a)		Christchurch	Older couple / Single	75+

IRD, Studylink government and no third party involved. Having to wait long on the phone.9(2)(a) Christchurch Older family 45-54 internal affairs because cyber crime is on the rise giving my details 9(2)(a) Auckland Younger family 45-54 registration renewal, DIA for online. 9(2)(a) Waikato Single 25-34 Vehicle registration 9(2)(a) Auckland

	Single	18-24	RealMe, Establishing my bona fides.		9(2)(a)	Auckland	Single	55-64	Contacting WINZ by phone		9(2)(a)	Auckland	Older family		55-64	IRD	information	9(2)(a)	Wanganui			
	Single	35-44	VTNZ	Not sure	9(2)(a)	Hawke's Bay		Older family			45-54	new UK passport			rather than completing forms			Duplicating info on forms			9(2)(a)	
	Auckland	Older family		45-54	Ird	process again		9(2)(a)	Auckland	Older family			45-54	ACC + immigration			Don't know	staff, staff often don't know info			9(2)(a)	
	Auckland	Younger family		25-34	NZ Transport		9(2)(a)	Wellington	Younger family		35-44	Vehicle registration			Nothing		Christchurch	Younger family			25-34	
	Single	18-24	RealMe, Establishing my bona fides.		9(2)(a)	Auckland	Single	35-44	NZTA	not sure	9(2)(a)	Auckland	Single	35-44	Ministry of Justice			I am not sure as I am not an IT expert.				
	Single	35-44	VTNZ	Not sure	9(2)(a)	Hawke's Bay		Older family			45-54	new UK passport			rather than completing forms			Duplicating info on forms			9(2)(a)	
	Auckland	Older family		45-54	Ird	process again		9(2)(a)	Auckland	Older family			45-54	ACC + immigration			Don't know	staff, staff often don't know info			9(2)(a)	
	Auckland	Younger family		25-34	NZ Transport		9(2)(a)	Wellington	Younger family		35-44	Vehicle registration			Nothing		Christchurch	Younger family			25-34	

IRD	Prevent acces by externa; parties and tighten up rules on online service providers	The amount of questions that didnt seem relevant	9(2)(a)		Waikato	Older couple / Single	55-64
Inland revenue		Having original copies of everything. They wouldnt take copies	9(2)(a)		Nelson	Younger family	25-34
ird	not sure		9(2)(a)		Auckland	Older couple / Single	45-54
Vehicle registration			9(2)(a)		Waikato	Older couple / Single	25-34
Msd, ird working for families		Finding time to sit down and do	9(2)(a)		Bay Of Plenty	Younger family	35-44
MSD		Time consuming	9(2)(a)		Christchurch	Younger family	25-34
My MSD, E-Services IRD		NA	9(2)(a)		Wellington	Older family	45-54
PASSPORT OFFICE		HAVING THE CORRECT INFO AT MY FINGERTIPS	9(2)(a)		Auckland	Younger family	45-54
Passports, Road Transport, Real Me,	Not sure but I would like assurance that my personal information is really secure	Ability to contact a real person when I became exasperated with the system	9(2)(a)		Taranaki	Older couple / Single	75+
Vehicle change of ownership		Providing proof of identity	9(2)(a)		Wellington	Younger family	25-34
Ird, acc,		Nothing	9(2)(a)		Christchurch	Younger couple / Single	25-34
IRD, ACC, MSD	Have a secure, encrypted online vault for the information which only can be accessed by certain people as required		9(2)(a)		Auckland	Older couple / Single	55-64
IRD	Solid passwords		9(2)(a)		Waikato	Older couple / Single	75+
ACC claim Rural Bonding Scheme withdrawal			9(2)(a)		Wellington	Younger couple / Single	25-34
Vehicle registration		Generally ok, just need to trust them.	9(2)(a)		Bay Of Plenty	Younger family	45-54
Tax agent forms			9(2)(a)		Bay Of Plenty	Older couple / Single	35-44

ACC, Immigration, IRD,		Difficulty in accessing NZ Immigration on 1 Occassion.	9(2)(a)		Auckland	Older family	55-64
IRD	Use finger print technology	Remembering	9(2)(a)		Wellington	Younger family	35-44
Doctor, IRD, ACC, Schools		Having to provide personel information.	9(2)(a)		Canterbury	Older family	45-54
NZ Post		Nothing	9(2)(a)		Waikato	Older family	55-64
wins	more security		9(2)(a)		Waikato	Older family	65-74
Gonappy		Nothing	9(2)(a)		Auckland	Younger couple / Single	18-24
Inland Revenue, DIA, High	Secure data so not easily hacked, two factor authentication in addition to	Having to provide same documents over and over again to diff	9(2)(a)		Auckland	Younger couple / Single	18-24
Ird & motor reg	Not divulge it to anyone.	Getting timely response.	9(2)(a)		Manawatu-Wanganui	Older family	75+
Vechicle association			9(2)(a)		Auckland	Older couple / Single	25-34
Change of car ownership, IRD services		Nothing really	9(2)(a)		Auckland	Older couple / Single	65-74
IRD	As much as it feasibly can		9(2)(a)		Auckland	Younger couple / Single	18-24
IRD		No problems	9(2)(a)		Wellington	Older couple / Single	55-64
Vehicle registration	Have photo ID checked.	none	9(2)(a)		Christchurch	Younger family	25-34
ird winz		nothing at all from memory	9(2)(a)		Otago	Younger family	25-34
IRD	Have personal contact with customer, not phone proms		9(2)(a)		Southland	Older family	65-74
IRD		I didn't find anything difficult	9(2)(a)		Auckland	Younger family	45-54

acc	regulation	steps	9(2)(a)		Auckland	Younger family	35-44
Passport Car Rego Tax Return	Avoiding unintended disclosure.		9(2)(a)		Wellington	Older couple / Single	55-64
Msd	More checks and secure systems		9(2)(a)		Waikato	Older couple / Single	65-74
IRD		Getting things set up in the first instance. Once that is done it is easy	9(2)(a)		Christchurch	Older couple / Single	55-64
						Younger couple /	
Transport Agency, IRD,	Make sure my details are encrypted and have someone qualified within government making sure that they remain private		9(2)(a)		Auckland	Older couple / Single	65-74
Social wellfare		Having not been given all the pass words.	9(2)(a)		Bay Of Plenty	Older couple / Single	65-74
Setting up IRD for our new son, PPL	More cyber security?	The RealMe login/website wasnâ€™t working properly	9(2)(a)		Auckland	Younger couple / Single	35-44
tax return	Keep personal information completely untouchable by a 3rd party		9(2)(a)		Auckland	Younger family	25-34
Passenger license			9(2)(a)		Waikato	Older couple / Single	55-64
IRD	Not allowing information to be shared between departments		9(2)(a)		Northland	Older couple / Single	65-74
DSW	Protected	Providing original to be	9(2)(a)		Bay Of Plenty	Older family	65-74
Acc		Clarity of	9(2)(a)		Auckland	Younger family	45-54
IRD		nothing	9(2)(a)		Tasman	Older family	55-64
Passport renewel		Proof of who I was.	9(2)(a)		Otago	Younger family	35-44
Tax Department	Making sure it can't be seen by anyone but them .		9(2)(a)		Auckland	Older family	45-54

Ird	Do not post anything anymore by mail.		9(2)(a)		Auckland	Older couple / Single	45-54
Passport office	Better security	Nothing major	9(2)(a)		Auckland	Older family	55-64
passport	making sure it's secure	nothing	9(2)(a)		Wellington	Younger couple / Single	25-34
land transport	enctypt it	proving you had authority to act	9(2)(a)		Canterbury	Older family	55-64
IRD, Work and Income	Better liasing with other Government departments which hold my details		9(2)(a)		Manawatu-Wanganui	Older couple / Single	55-64
NZTA to change registration on a			9(2)(a)		Waikato	Younger couple / Single	25-34
Work and Income	By not being able to allow others to gain this information		9(2)(a)		Wellington	Older couple / Single	75+
For a passport Court			9(2)(a)		Gisborne	Older couple / Single	65-74
			9(2)(a)		Auckland	Older family	25-34
immigration	have a secure website that is easy to understand. It appears the sites are designed by computer people but they never get tested by the public		9(2)(a)		Wellington	Older couple / Single	65-74
health, NZTA		EXPLAINING THE ANSWER WAS SEEKING.	9(2)(a)		Waikato	Older couple / Single	75+
MyIR, NZTA	Ensure end to end encryption	Too many hoops to jump through	9(2)(a)		Auckland	Younger family	35-44
Ministry of Social Development - Study Link, Real me etc			9(2)(a)		Christchurch	Younger couple / Single	18-24
Withdrawal of Kiwisaver to buy first home		Time involved	9(2)(a)		Christchurch	Younger family	35-44
IRD		Having to use lawyers to verify my POA and repeatedly having to prove my identity	9(2)(a)		Christchurch	Older couple / Single	55-64
Ird tax return NZ high commission in London			9(2)(a)		Wellington	Younger couple / Single	25-34

Nzta,	Unsure of details		9(2)(a)		Wellington	Younger couple / Single	25-34
DHB, ACC			9(2)(a)		Canterbury	Older family	35-44
Acc	Inform people of where personal information goes and how it's used		9(2)(a)		Christchurch	Younger couple / Single	25-34
IRD		scanning in documents - sometimes too large	9(2)(a)		Waikato	Younger family	35-44
NZTA ACC		Navigating the website and understanding what it was asking for	9(2)(a)		Auckland	Older family	45-54
Department of Internal affairs		Remembering login	9(2)(a)		Wellington	Younger family	25-34
Vehicle			9(2)(a)		Waikato	Younger couple / Single	18-24
IRD			9(2)(a)		Wellington	Older couple / Single	75+
		Using personal details to vouch for				Older couple /	
acc	not sharing it	lack of instructions	9(2)(a)		Auckland	Older couple / Single	55-64
IR, ACC,		Filling in forms	9(2)(a)		Wellington	Younger family	55-64
Winz, IRD, Statistics nz	Keeping it secure via SSL as well as 2FA and probably other layers of security. Government employees that breach privacy laws should be prosecuted as well.		9(2)(a)		Christchurch	Younger couple / Single	25-34
NZ Transport Agency		Nothing	9(2)(a)		Otago	Younger family	35-44
ird	more security		9(2)(a)		Wellington	Younger couple / Single	25-34
Vehicle registration		Nothing	9(2)(a)		Auckland	Younger family	35-44
Reigstering a vehicle, Tax Return			9(2)(a)		Auckland	Younger couple / Single	18-24

Registration of motor vehicle			9(2)(a)		Auckland	Older family	75+
Tax			9(2)(a)		Christchurch	Younger couple / Single	18-24
Car rego, IRD tax		Not quite sure what you're asking me here	9(2)(a)		Northland	Older couple / Single	45-54
Vehicle Registration, Passport Renewal		The criteria required to meet some of the requirements is getting out of hand	9(2)(a)		Auckland	Younger family	35-44
Realme	Because		9(2)(a)		Wellington	Older family	25-34
Study link, myird, real me	Make it more secure		9(2)(a)		Northland	Younger couple / Single	18-24
Winz	I don't understand the technology involved and that makes me suspicious of how safe my information is.		9(2)(a)		Canterbury	Older couple / Single	65-74
Internal Affairs	Heavily encrypted two stage process	Nothing really, the security systems can be tripped in some cases if you tried hard enough	9(2)(a)		Auckland	Older family	65-74
ACC	J		9(2)(a)		Christchurch	Younger couple / Single	18-24
Winz, New Zealand Police	keeping as little as possable information online	proving that I was acting on a perons behalf	9(2)(a)		Southland	Younger couple / Single	45-54
Immigration NZ Inland Revenue Companies Office		Nothing apart from the departments				Older couple /	

New Zealand Transport Agency Time to find and collate the information 9(2)(a) Northland Younger family 45-54 Register a vehicle urne my name Not sure 9(2)(a) Marlborough
Single 18-24 Ird company business 9(2)(a) Auckland Single 55-64 ACC crappy system 9(2)(a) Auckland Single 45-54