



November 2019

.nz survey - summary and analysis

InternetNZ

Photo by [Bench Accounting](#) on [Unsplash](#)

Table of Contents

Purpose	2
Background	2
Key points of survey findings	2
How to read this paper	6
Security	9
Openness	16
Access	20
Privacy	23
Te Tiriti and Te Reo Māori	27
Human Rights	31
Business	34
What else respondents would like us to know	38

Purpose

To provide the .nz Advisory Panel with our analysis of the online .nz survey ('survey') results and summarise key findings. We intend that these key findings can help you with your evidence base to underpin the issues for your report.

Background

The survey ran for four weeks from September to October 2019. 276 New Zealanders responded to the survey. The questions were a mix of closed and open questions covering the issues and lenses the Panel has been discussing (security, openness, access, Te Tiriti and te reo Māori, privacy, e-commerce and human rights).

In the Google shared drive, we have put a complete collection of the:

- raw survey data including the open-ended responses;¹ and
- InternetNZ-generated diagrams from that raw data.²

Key points of survey findings

Below are some key findings from the survey that may be useful for your .nz policy review work.

Security: mixed response on how secure .nz is but consensus over greater awareness raising to increase confidence

1. A number of respondents felt .nz is **secure** (36%), yet many also felt it is not secure, somewhat secure or has average levels of security (43%) with a fair number who didn't know (21%).
2. Many respondents submitted they have been the victim of a **phishing** attack (43%) from a .nz domain or other domain name. Over half (55%) of respondents have not been a victim of a phishing attack. (Some may have interpreted the question to be that they had received a phishing email rather than lost money to an attack.)
3. Some concern exists amongst those who answered the open-ended questions about the increasing number of phishing attacks but most said that attacks

¹ "02.2 .nz Panel survey results - excel"

<https://drive.google.com/open?id=1aJBl3Ha6bIKSkhO75pEDEr7kiCy8SQIJFQw71NLX8>

² <https://drive.google.com/open?id=1pPxbNFN7PaJOLhvl6obNF9ituCi7ibJc>

are often obvious (e.g. misspellings, etc) and they tend to “come from” major entities (e.g. IRD, BNZ, NZ Post, Westpac).

4. Many people think greater awareness of the security measures taken by InternetNZ (including legal action) would increase **confidence in the security of .nz**. A few thought stronger verification of registrant details may increase trust. As seen at the Panel’s Nethui event, some respondents advocated for greater visibility of registrant details (WHOIS) but others thought registrant details needed greater protection. A few noted how difficult it is to overcome hackers who will always get around the system, one noted NZ firewall and another proposed stricter requirements by registrars for DNSSEC.

Openness and access

5. Most respondents (65%) didn’t know if .nz is as **open** as it needs to be, a fair share (28%) thought it is as open as it needs to be and the minority (8%) thought it is not as open as it needs to be.
6. The majority of people did not consider there were **barriers** to using .nz (60%), many (34%) didn’t know. Price was raised as both a barrier to access, and a barrier to openness. Respondents thought that businesses not using a .nz domain may have a variety of reasons for not doing so. Reasons included low awareness, a lack of skills, or because other domain names were cheaper.
7. Nearly half of the respondents (44%) don’t know if the people who want or need to **access** .nz have access to it. A fair share of respondents (38%) think that people do have access to .nz domain names if they want or need them.

Privacy: respondents are divided on enhancing privacy options

8. A large number (29%) of respondents were unsure if there are **privacy** issues in using a .nz domain. A significant proportion of respondents (52%) submitted they’ve never personally had any privacy issues in using a .nz domain name. Some submitters (18%) had experienced privacy issues.
9. For the open-ended question on privacy, a number of respondents (13 of 71), including many who hold .nz domain names, were concerned their details (particularly physical address and phone number) are freely available online. Some admitted they’ll put in a PO Box or fake details to protect themselves. A few asked for proper protection of vulnerable groups (including transgender people).³ However, a few noted privacy has improved with the introduction of the Individual Registrant Privacy Option (IRPO). Some respondents were concerned that closing off information from WHOIS encourages abuse of the

³ This was submitted under the human rights question but is relevant under privacy.

DNS by limiting oversight. A few considered the privacy issues will not be any different to those experienced overseas. (You'll recall this tension in opinion also arose at the NetHui session.)

Te Tiriti and use of te reo Māori: opinions were divided

10. Over half of respondents (55%) consider it is important or extremely important to protect the appropriate use of **te reo** in managing .nz.
11. In the open-ended question, some believe .nz should enable Māori words to enable dignity and worth, support Māori⁴ and that te reo represents NZ. One respondent raised that .iwi was created for this purpose. One respondent noted .nz is not the Māori name for NZ. Many others felt all languages should be considered, not only te reo.
12. Responses canvassed on the management of .nz reflecting the **partnership intent from Te Tiriti** included a range of views:
 - a. many people believe NZ is bi-cultural, Māori should be involved in the process, .nz is a taonga, greater diversity in INZ staff would help, and it is respectful to include the principles in the .nz policies
 - b. many other submitters found it challenging to see how Te Tiriti is connected or relevant to the modern domain name space. Others felt that enabling Māori words on .nz would be a sign of special treatment and felt everyone should be treated equally
 - c. many submitters felt insufficiently qualified to respond and advised to consult Māori directly (iwi, hapu, whanau).

Human rights: respondents believe human rights are important but that hate speech and abuse are unacceptable

13. The majority of respondents (80%) think human rights are important or extremely important for .nz. The minority (3%) consider human rights are not important and a few (13%) considered they were somewhat important.
14. Respondents consider human rights are important for democracy but many consider safety (against hate speech or bullying) is paramount but that there is a fine line to navigate. Most submitters viewed human rights through a lens of free expression.

⁴ This submission was made under the general catch-all question (Q16).

15. Submitters diverge on how human rights should be applied. Of 80 open-ended responses:
- a. About 11 think free expression should be protected at all costs
 - b. About 35 consider free expression should be protected but not if harm will occur (hate speech and violence)
16. A small number of respondents (2) think InternetNZ should hold a position against hate speech and abuse on .nz. A small number (2) want to see .nz be a neutral service; not making content decisions.

Supporting businesses: respondents see the policies as a part of what causes businesses to flourish or be hindered online

17. Many respondents (52%) consider the .nz policies are important or extremely important to **support or hinder NZ businesses** to flourish.
18. Some respondents consider it is essential the policies support business needs and foster high trust and security in .nz to maintain its credibility with local consumers. A .nz domain is central to branding a NZ business. Lowering barriers to access (affordability, skill levels) for business is important and liaison with NZBN⁵ is needed. However, others did not see it as a priority, felt it should be left to business leaders, or felt business is complex so factors won't be solely based on the .nz policies. Others felt .nz is too small if a person wants a global business (so .com is attractive). (You'll recall similar opinions were expressed in the UMR research.)

⁵ The New Zealand Business Number,
https://www.nzbn.govt.nz/?gclid=EAlaIQobChMIy7Di9f7i5QIVRqqWCh3YHQOyEAAAYASAAEglnfD_BwE

How to read this paper

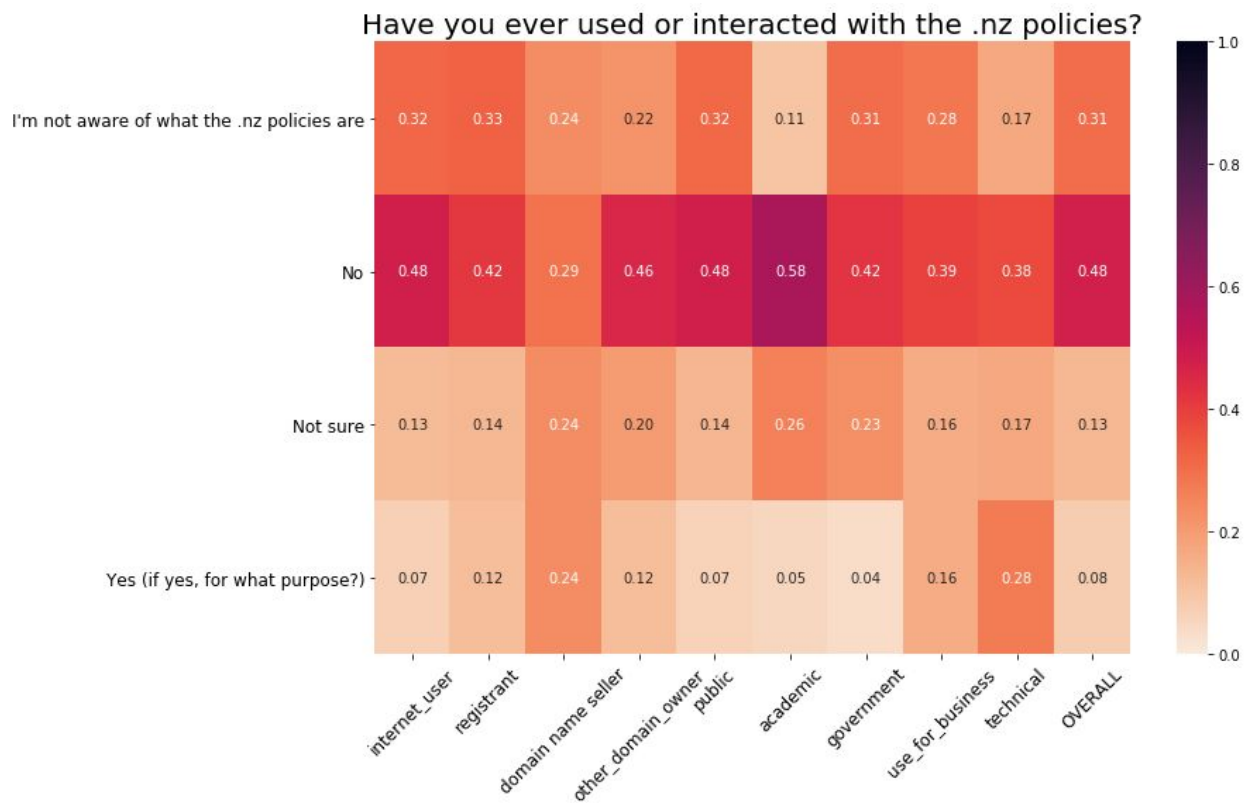
This paper is a review of the responses to both the closed and open ended questions in the survey. Below is a guide to how we have approached the analysis and presented the information.

Diagrams and data analysis

Our data team has helped us to crunch the raw data from the survey results.

The team has generated diagrams to show the fraction of each user type from each closed survey question (see Figure 1 below). For instance, the diagram below reflects the question posed in the survey: “Have you ever used or interacted with the .nz policies?”

Figure 1: Distribution of answers per respondent type for question 'have you ever used or interacted with the .nz policies?'

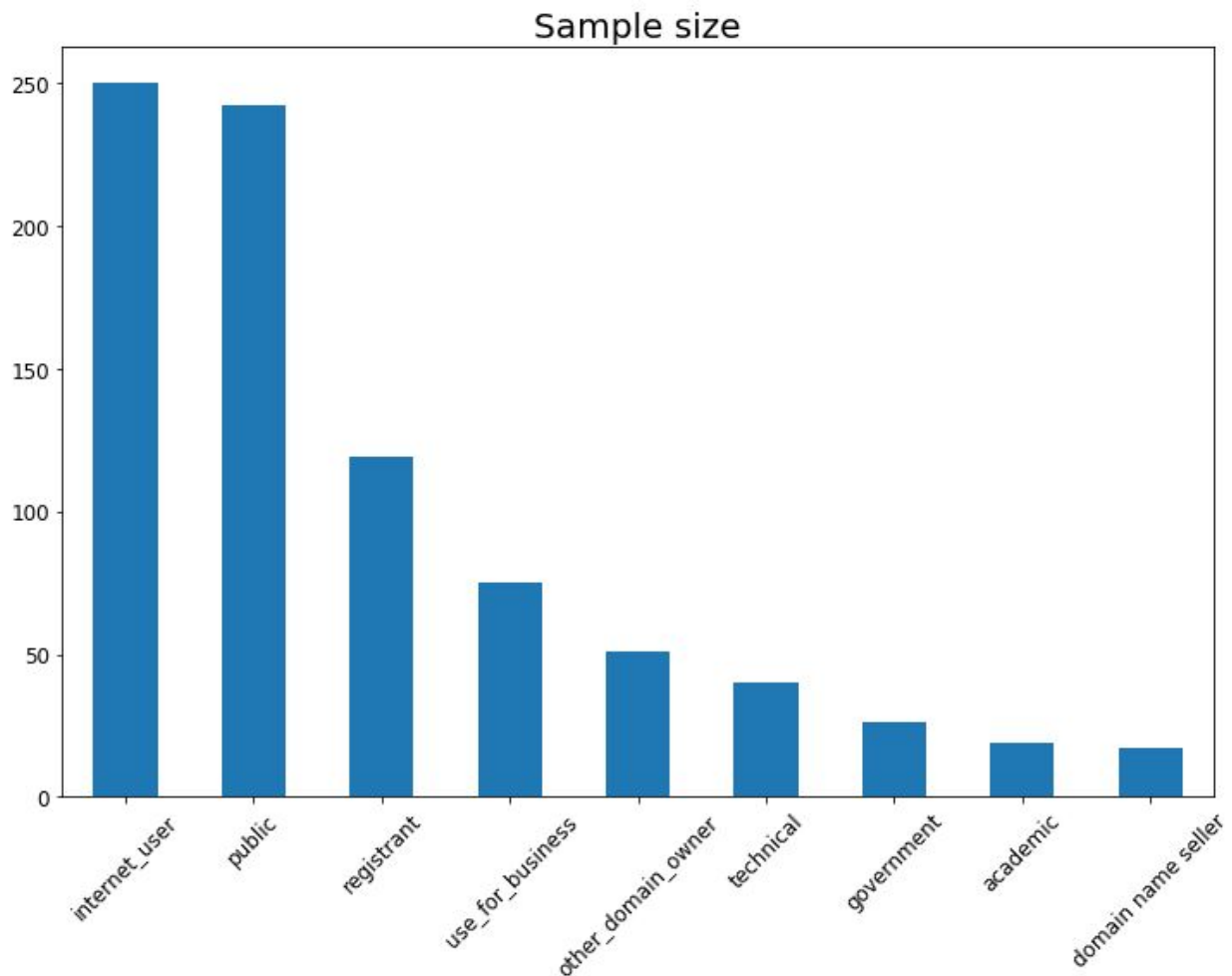


Each column represents a group of respondents (e.g. “academics”), as well as their responses to the question. Each column adds up to 1. The rightmost column is calculated on overall respondents.

Note that survey respondents could select which group they belonged to, which could result in being tagged to more than one group. This means a user who is a member of the public and also a registrant will have their closed question response counted in each section.

User groups were unequally represented. Below is a bar chart (Figure 2) which shows how many of each user type answered the survey.

Figure 2: Number of respondents based on internet usage and professions.



Analysis of open ended responses

We have themed and categorised all responses to the open-ended survey questions and drawn key findings from those responses in this paper. Not all respondents answered each open-ended question in the survey. The number of responses varied for each question - the minimum was 29 and the maximum was 161. We also found some responses were not directly relevant to the .nz policy review as they reflected

upon wider Internet issues - we have limited these indirect responses from our analysis.

In our analysis we tend to focus on the type of respondent (i.e. registrar or registrant) and their response.

Security

How secure do you think .nz is?

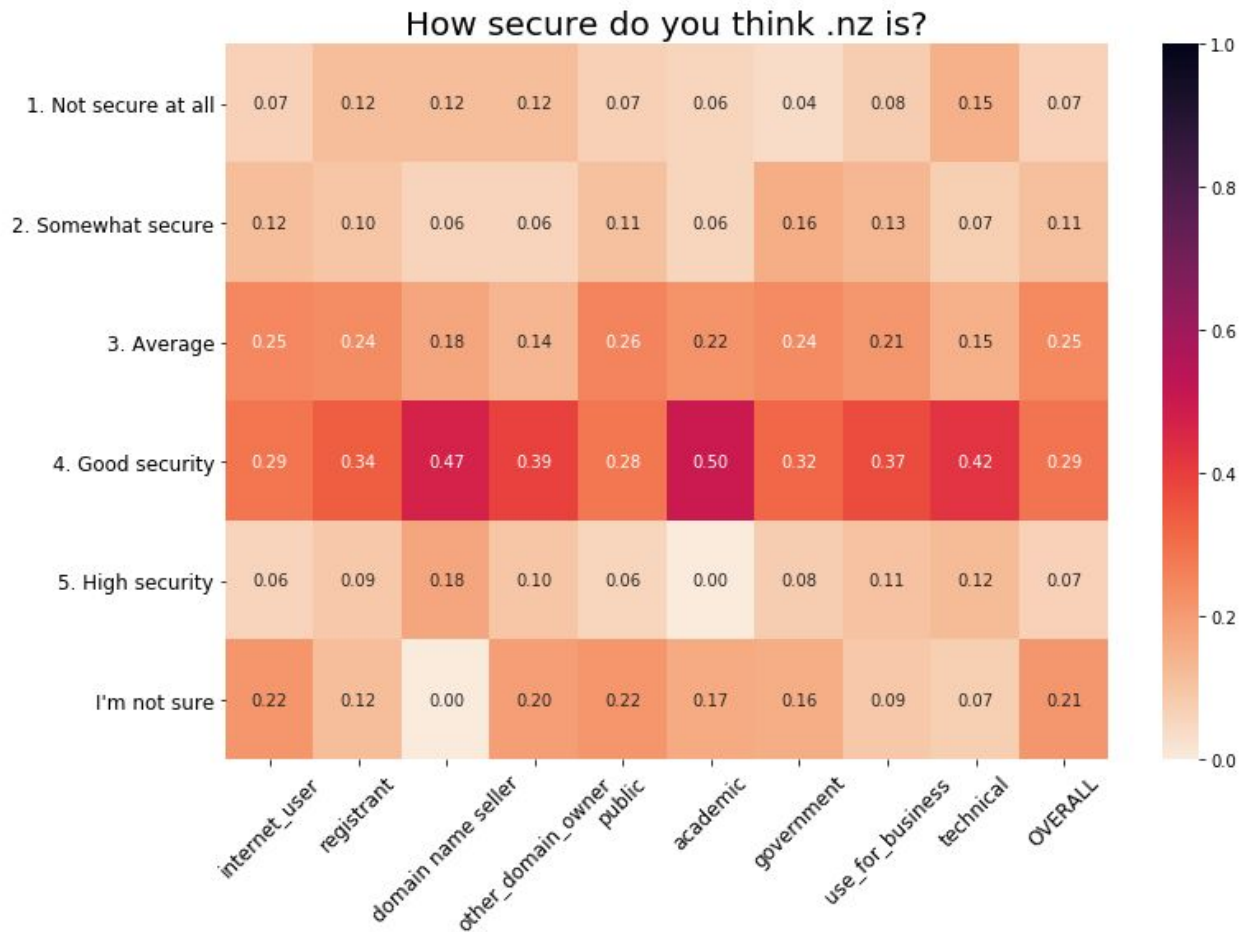
Below is a bar chart (Figure 3) of the closed question to the survey, 'how secure do you think .nz is?'.

Figure 3: Distribution of answers for the question 'how secure do you think .nz is?'.



The next diagram (Figure 4) shows how each type of respondent considered the security of .nz.

Figure 4: Distribution of answers per respondent type for question 'how secure do you think .nz is?'



Key findings:

The responses to this question show respondents think largely positively about how secure the .nz domain name space is. 25% of people thought the security of .nz is “average”, and 36% of people thought .nz security is “good” or “high”. A fairly large number of respondents answered that they were not sure (21%). Those who sell domain names, or are technical, are largely confident in the security of .nz. Those who hold other non- .nz domain names also thought security of .nz was “good”.

What would increase your confidence in the security of .nz?

We had 142 responses to this open ended question. We have categorised these responses below, providing you with a high level overview.

Many people don't know much about security but want greater awareness

1. Approximately 37 out of 142 people said they did not know how to improve their confidence in the .nz domain name space.
 - a. 30 of these 37 people said they did not have enough information to offer an opinion
 - b. Seven people thought nothing could be done because online security threats were an unavoidable risk of being online
2. Many of the responses conflated websites with domain names, or thought the government administers .nz domain names, so their comments were not directly relevant to the security of .nz. For example, a few people wanted to see greater use of HTTPS to improve security. While this is a good Internet security measure, it is unrelated to .nz policies.

Visible security failures negatively affect confidence in .nz

3. A few people responded specifically about scammers and phishers who use .nz. These people wanted to see .nz free of scammers to increase their confidence in .nz. There was a lot of suspicion towards email as a security threat in general.
4. A few people appeared to think the government ran .nz, and therefore the public security breaches suffered by government websites created doubt in the security of .nz: *"The hack of the labour governments website made me lose a bit of faith! (Where they got access to the upcoming budget)."* [sic]

Visible action and success positively affect confidence in .nz

5. 20 respondents thought that evidence of security measures, and publicity about steps taken to make .nz more secure would increase confidence.
6. A further 20 people thought more awareness about what InternetNZ is and the work we do would improve confidence.
7. One respondent called for *"Regular information releases on security status, breaches and initiatives"*.

Some people want to see registrant verification and local presence requirements

8. Amongst those who expressed low confidence in the security status of .nz currently (38 people), five people said a local presence requirement would improve confidence if all .nz domain names were registered by New Zealanders.
9. Around 10 people suggested that verification of registrant details, and cancellation of any domains with false registration details would increase their confidence in the .nz space. To increase confidence, *“[I want to] know that any domains with .nz have been independently verified and that their activities are audited and regulated.”*

Views on the impact of making registrant details public is mixed

10. Some people thought that hiding registrant details was good for security, and others thought it was bad for security.
11. For some, confidence in the .nz domain space meant that their privacy as a registrant was protected: *“[I want the...] ability to hide ALL my [details] and companies details regarding the ownership of domains.”*
12. For some, the ability to interrogate domain name registrant details was critical: *“[I want to be] able to see, via a 'whois' query (ie, with the long standing tool, TCP/43), who has registered a domain and where they are based (eg, "April Smith, Wellington, New Zealand"). This detail, while generally still available for .nz, is now difficult to obtain (requires a web browser, and answering one or more captchas, making it difficult to look for correlations in registrations).”*

Some people would feel more secure if they had more support, from either InternetNZ or their community

13. A few people said their confidence would be increased if they knew where to turn for help when they did not know something about .nz or the Internet more broadly.
14. One respondent wanted someone in their community or family they could turn to for support: *“A whanau member on .nz whom I trust to inform me daily and let me know how to prevent, detect, quarantine, clean and update my entire system, where and when needed.”*

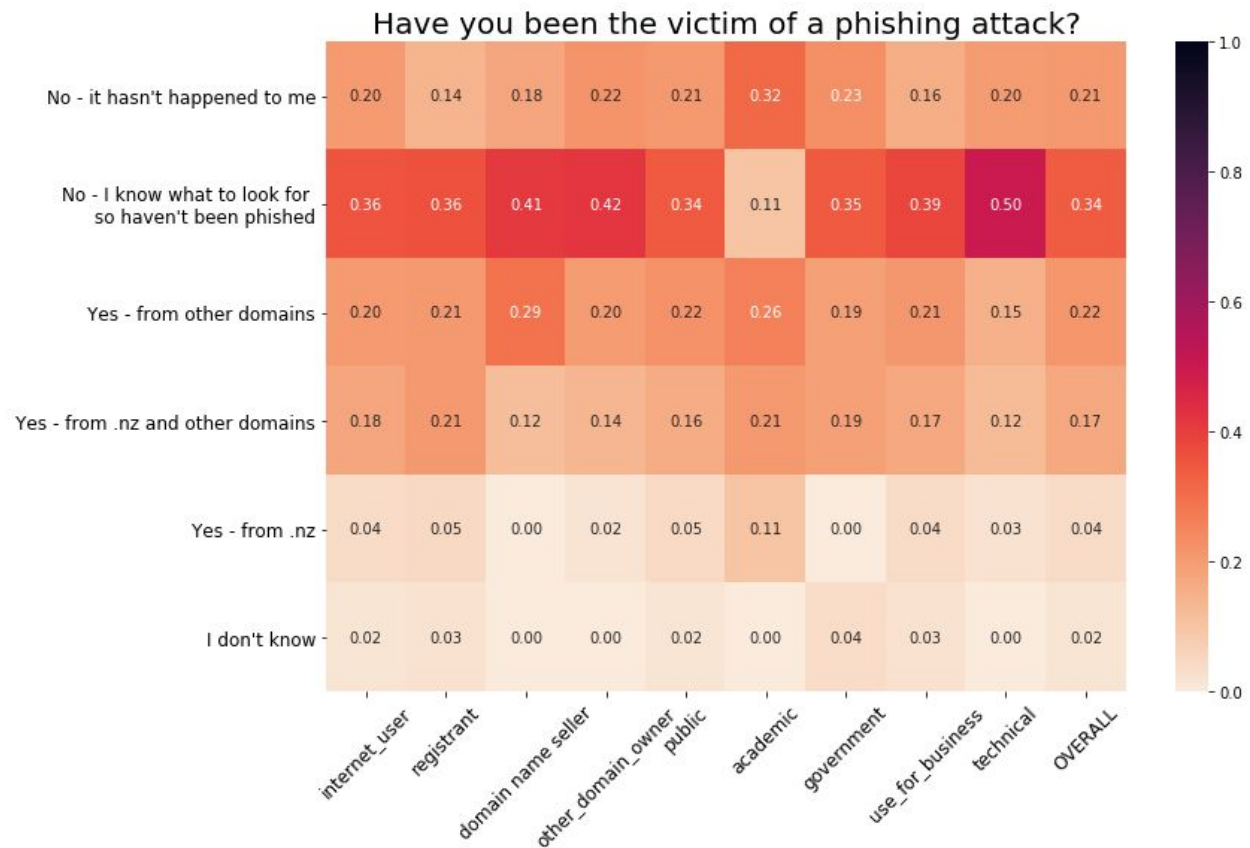
A few people said that increasing security of .nz would mean making trade-offs regarding ease of registration

15. A few strong opinions came through about whether improving security or requiring user verification would negatively impact the ability of people to use .nz.
16. From one registrant: *“I don't think the security of all .nz domains could be better without excessively restricting the ease of registering a domain. I'm not sure InternetNZ can/should really enforce any security assurances for all .nz domains.”*
17. A technical respondent submitted: *“I'm not convinced that the domain registration system is the right place to be implementing fraud, spam, illegal streaming, and security exploits. I think the NZ domain system should be engaged with the global DNS community on improving security (though DNSSEC seems pretty dead in the water, wouldn't recommend that).”*

Phishing

Below is a bar chart (Figure 5) showing the closed question to the survey on the topic of phishing attacks.

Figure 5: Distribution of answers per respondent type for question 'have you been the victim of a phishing attack?'



18. In the survey, we asked respondents “Have you been the victim of a phishing attack”? Those who answered yes were asked to provide more information. We had 94 open ended responses.

19. Most respondents (66) have not been the victim of a phishing attack, rather they report that they recognise phishing emails and receive them often.

20. Only 3 respondents said they have been the victim of a phishing attack. One was via TXT. Another was a targeted phishing attack known as “spearfishing”. And another was phished but they did not say how. A few others (2) mentioned being hacked, but did not describe how.

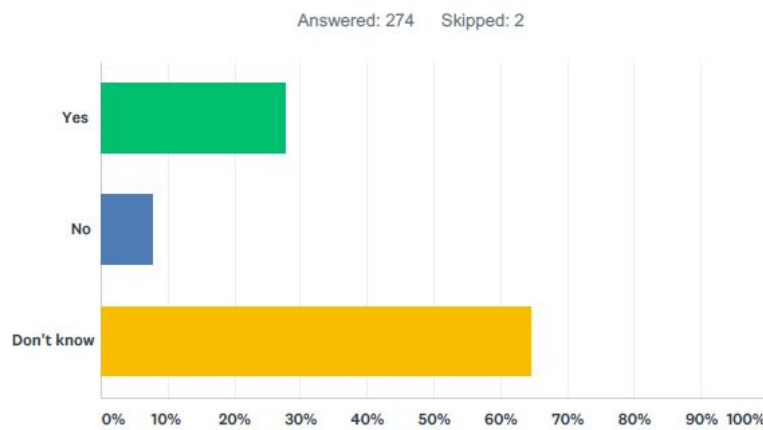
21. 10 respondents mentioned receiving phishing emails that looked like they were from government agencies, most often from IRD.
22. Overall, respondents talk about receiving a lot of phishing emails, but can recognise them and they are either filtered automatically, or people know to ignore them.

Openness

The chart below (Figure 6) shows sentiment across all respondents on the openness of .nz.

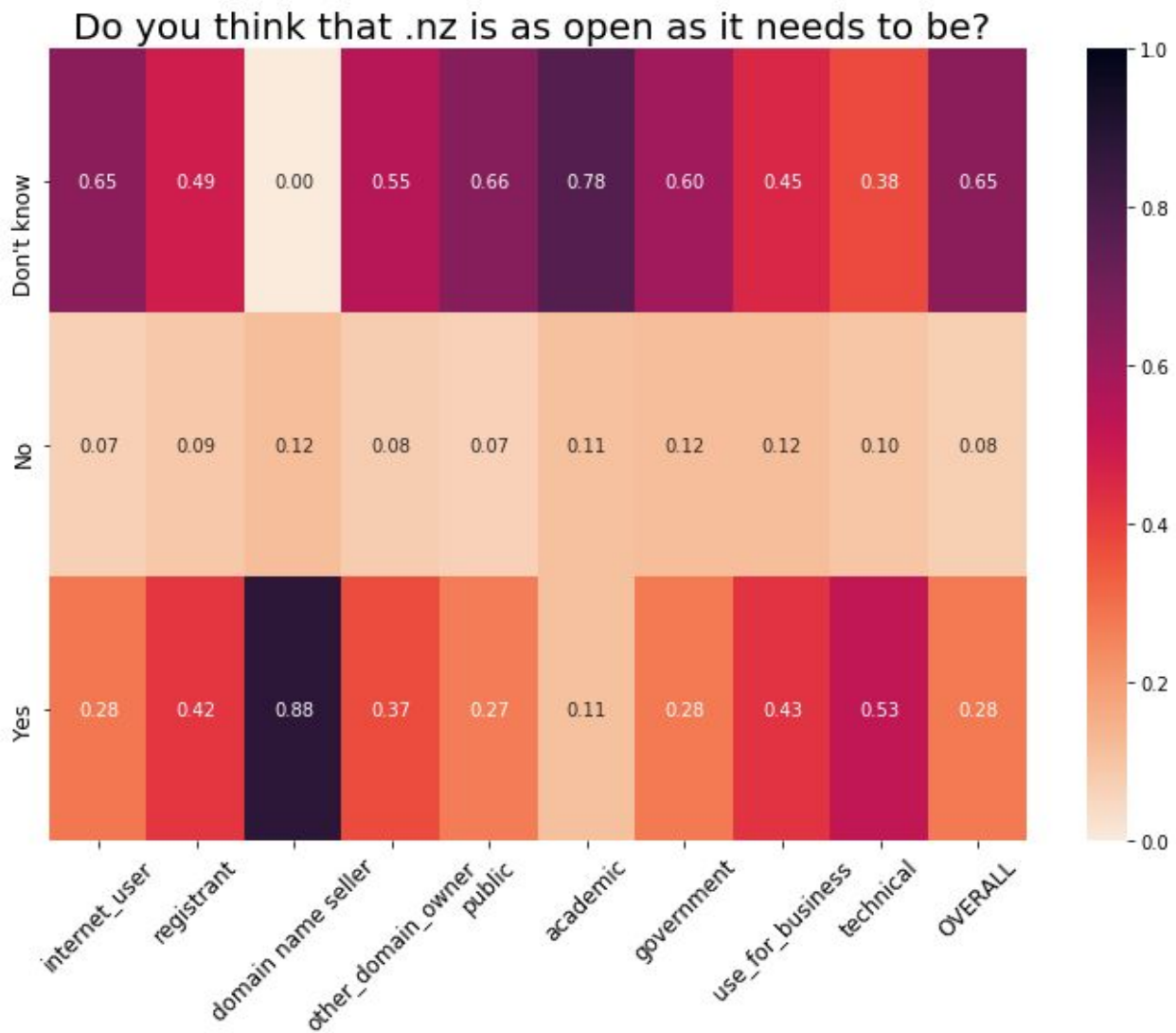
Figure 6: Distribution of answers per respondent type for question 'do you think that .nz is as open as it needs to be?'

Q7 Do you think that .nz is as open as it needs to be? (By open, we mean whether .nz supports people to participate online, to create new uses of .nz and to innovate).



ANSWER CHOICES	RESPONSES
Yes	27.74% 76
No	7.66% 21
Don't know	64.60% 177
TOTAL	274

Figure 7: Distribution of answers per respondent type for question 'do you think that .nz is as open as it needs to be?'



Key findings:

The majority of respondents (65%) do not know if .nz is as open as it needs to be. Some considered it is as open as it needs to be (28%). A minority considered .nz is not as open as it needs to be (8%). Those who sell domain names overwhelmingly consider .nz to be as open as it needs to be (88%). Academics and other domain name holders were the groups with the highest response rate that they didn't know.

Open ended question: Please share more about your answer here

The open ended question asked if .nz is as open as it needs to be, which 48 respondents answered. We also asked respondents to identify any barriers to using .nz, which 29 respondents answered.

Most people who responded considered price a barrier

1. A third of those who answered the question considered price a barrier. Some mentioned that gTLDs (like .com) are often cheaper.
2. Some of the respondents considered the cost of maintaining a web presence, including email hosting and website development, too high and the barrier to entry was too great.
3. From one participant: *“Cost, need for technical expertise and separate steps create attitudinal barriers. User needs domain, hosting, web construction and ongoing maintenance. All cost and have technical requirements. Cheap or free out of the box options would help overcome this.”*

Respondents who do hold an opinion largely thought .nz was open

4. Of those who answered yes or no, as to whether .nz is as open as it needs to be, most answered yes (28% compared to 8% answering ‘no’).
5. Three respondents thought .nz was too open, as it permitted domain name confusion and use of domain names to cause harm.
 - a. *“.nz is one of the most open TLDs in the world, arguably too open (eg, having abandoned any 2LD hierarchy restrictions, but retained them in parallel, which can lead to confusingly similar names -- example.co.nz and exampleco.nz, for instance).”*
 - b. *“A little too open with overseas parties being able to masquerade as being based in NZ for nefarious reasons.”*

Respondents believe opportunities exist to work better with communities

6. A few respondents offered ways that .nz could better communicate openness:
 - a. One thinks we should work with the Māori and New Zealand Sign Language (NZSL) community
 - b. Three think we should be doing more brand awareness work
 - c. One stated that .nz is exclusionary of minorities, but did not explain this comment.
 - d. One registrant and technical person thought we should work with the Internet community: *“I would like to see .nz operate closer with the internet community, similar in the way CertNZ are raising security awareness for companies and reaching out via educating consumers.”*

There are myths about .nz domain names

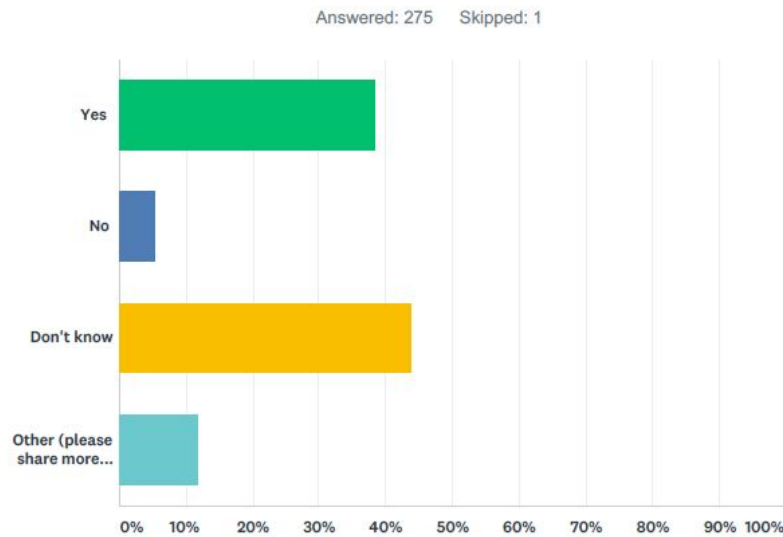
7. The question about barriers to access revealed some myths about the .nz domain space. This suggests that more awareness raising is required. Below are myths that have come up in this section.
 - a. **.nz is more expensive than .com:** a number of respondents mentioned that .com is cheaper than .nz. While some registrars do offer .com names at a lower cost, many offer .nz and .com names for the same cost.
 - b. **.nz cannot be global:** *“.nz to Google is a New Zealand business and is indexed as such. Using Google Search Console/Analytics .com can be identified with any country. (I stand to be corrected, as the Internet changes rapidly)”*
 - c. **A New Zealand presence is required:** *“You must be based in New Zealand”*
 - d. **.co.nz is distinct from .nz:** a few respondents thought the survey was asking them about .nz in opposition to .co.nz. This appeared in answers for other sections as well.
 - e. **There are verification checks:** *“It is nearly 20 years since our .org.nz address was registered so I can't remember how much information we needed to provide, but I am sure some checks were made about our status as an organisation.”*

Access

The chart below (Figure 8) shows sentiment across all respondents in terms of access to .nz.

Figure 8: Distribution of answers for question 'do you think the people who want, or need, to access .nz have access to it?'

Q9 Do you think the people who want, or need, to access .nz have access to it? (By access we mean people who want a .nz domain name can afford it and have the knowledge/skills to set it up and use it.)



ANSWER CHOICES	RESPONSES
Yes	38.55% 106
No	5.45% 15
Don't know	44.00% 121
Other (please share more about your answer here)	12.00% 33
TOTAL	275

Figure 9: Distribution of answers per respondent type for the question 'do you think the people who want, or need, to access .nz have access to it?'

Do you think the people who want, or need, to access .nz have access to it?



Key findings

1. This question divided respondents:
 - a. Most answered “yes” (38%) or “don’t know” (44%) suggesting that those who are familiar with .nz consider it to be accessible
 - b. A small minority of respondents (5%) answered “no” - people do not have access if they want or need it. Notably some (12%) responded “other”.
2. Registrants, domain name sellers and technical people were more likely to consider .nz to be accessible, whereas those from government, academia, and general Internet users were more likely to not know.

Opened ended response on access

Only those who answered “other” got the opportunity to answer the open-ended question, and there were 34 responses. The key insights are below:

Having a web presence is complicated for those who are not technical

3. About one third of those who responded to the open-ended answer cited a lack of knowledge or awareness about how to use domain names as a barrier to accessing .nz.
4. One non-.nz domain name holder stated many businesses stick to Facebook and Gmail: *“Knowledge/skills for hosting etc aren't common place, and it's complex to unpack (if you're particularly safety conscious/want to get it right). Too many NZ businesses use gmail and Facebook for *all* of their web presence.”*

gTLDs are perceived as cheaper, easier and better for global branding

5. Some respondents stated that .com seems cheaper and easier to access, and helps position a brand globally.
6. One registrant commented about the perception of cost: *“.nz is generally more expensive than say .com and that could be a barrier, even if only a perceived one.”*

People would like more information and education about .nz

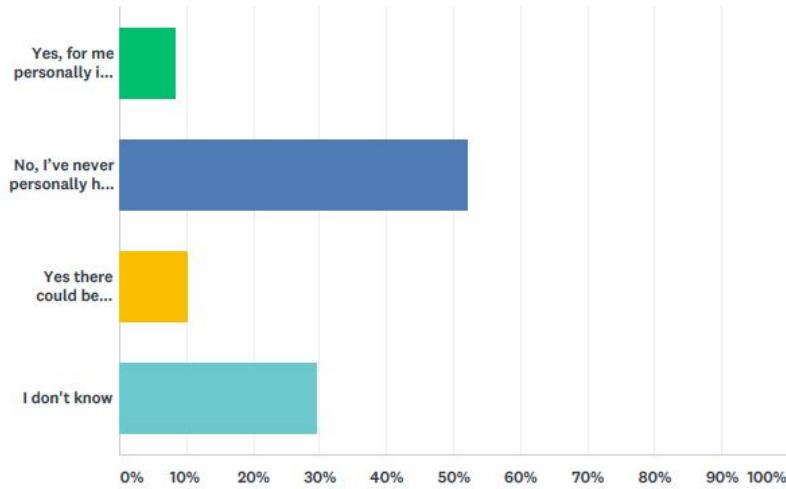
7. From someone who works for a registrar: *“Especially in the domain space, people need constant refresher updates as things change, eg. privacy laws, DNS security, WHOIS privacy settings, domain name locks, 2FA etc. Would be nice to work closer with online communities like eg. Geekzone, join the events where tech experts meet up. Provide guest speakers etc.”*

Privacy

Figure 10: Distribution of answers for question 'do you think there are any issues with your privacy in having or using a .nz domain name?'

Q10 Do you think there are any issues with your privacy in having or using a .nz domain name?

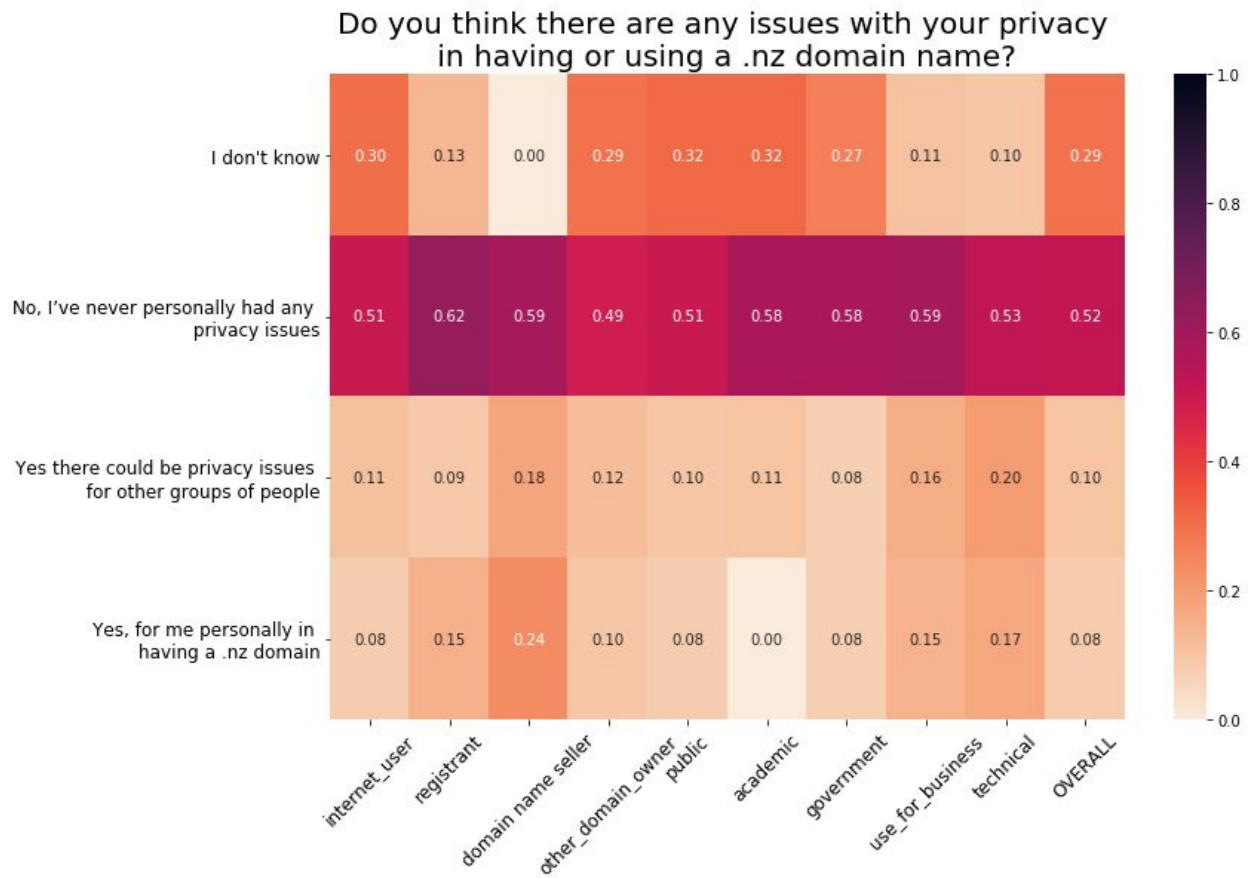
Answered: 275 Skipped: 1



ANSWER CHOICES	RESPONSES	
Yes, for me personally in having a .nz domain	8.36%	23
No, I've never personally had any privacy issues	52.00%	143
Yes there could be privacy issues for other groups of people	10.18%	28
I don't know	29.45%	81
TOTAL		275

The next diagram shows how each type of respondent considered the privacy status of the .nz domain name space.

Figure 11: Distribution of answers per respondent type for question 'do you think there are any issues with your privacy in having or using a .nz domain name?'



Key findings

Domain name sellers, businesses and technical people were more likely to consider there were privacy issues in having a .nz domain name than government or academics. Overall, most respondents had not experienced privacy issues (52%). A high number of respondents (29%) were not sure. This suggests people have either not considered or do not know about privacy issues related to the .nz domain name space.

What are the privacy issues you see (if any)?

71 people out of 276 people responded to the open-ended question: “What are the privacy issues you see (if any)?” We summarise the key insights below:

Many respondents are worried about their personal data online.

1. Some respondents focused on their fears about tracking and data breaches across the Internet (not specifically just .nz) that would put their personally identifiable information (PII) at risk.
 - a. At least 14 of the 71 responses mentioned fears about the protection of their personal information specifically.
2. One respondent noted regarding privacy concerns that they see *“particularly for shopping sites, quite a bit of information is gathered and stored such as addresses, phone numbers, email addresses, gender, shopping preferences etc. If someone were to hack a site they could use or sell this information which can be used to lure someone into a scam.”*

Many respondents are concerned with the openness of WHOIS

3. Some respondents, including many who hold .nz domain names, were concerned that their details were freely available online through WHOIS. At least 13 of the 71 respondents who answered specifically raised issues with WHOIS.
4. A domain name seller and technical person submitted: *“The biggest issue for me is that a lot of people have personal info in WHOIS without realising it's world-readable and permanently out there. People might expect it's fine for now but not expect the long term impact.”*

A few respondents were concerned about misuse of the IRPO, and the ability to mask registrant information in WHOIS

5. About 8 of 71 respondents expressed views that closing off information from WHOIS encourages abuse of the domain name system, and limits oversight.
6. From a technical sector respondent and domain name holder, *“I have a problem with TOO MUCH privacy: I can't get my 'technical contact' information published in the whois service. The suppression of registrant details means we no longer have a feedback loop to enforce the quality of data in the registry [...] There are ineligible entities holding private registrations, and because nobody can check them, they get away with it.”* [sic]
7. Another technical sector respondent, who holds several domain names, was extremely concerned about potential abuse of the Individual Registrant Privacy Option (IRPO): *“The IRPO seems to be massively abused by non eligible entities using this option. While I think IRPO is required for domain names owned by individuals their needs to be some process involved that checks eligibility.”*

8. [note from InternetNZ] It should be noted that InternetNZ does not have evidence of 'massive' abuse, but there are instances where organisations have been able to activate the IRPO, and InternetNZ would follow up any specific complaints.

There is a reasonable path to privacy for registrants

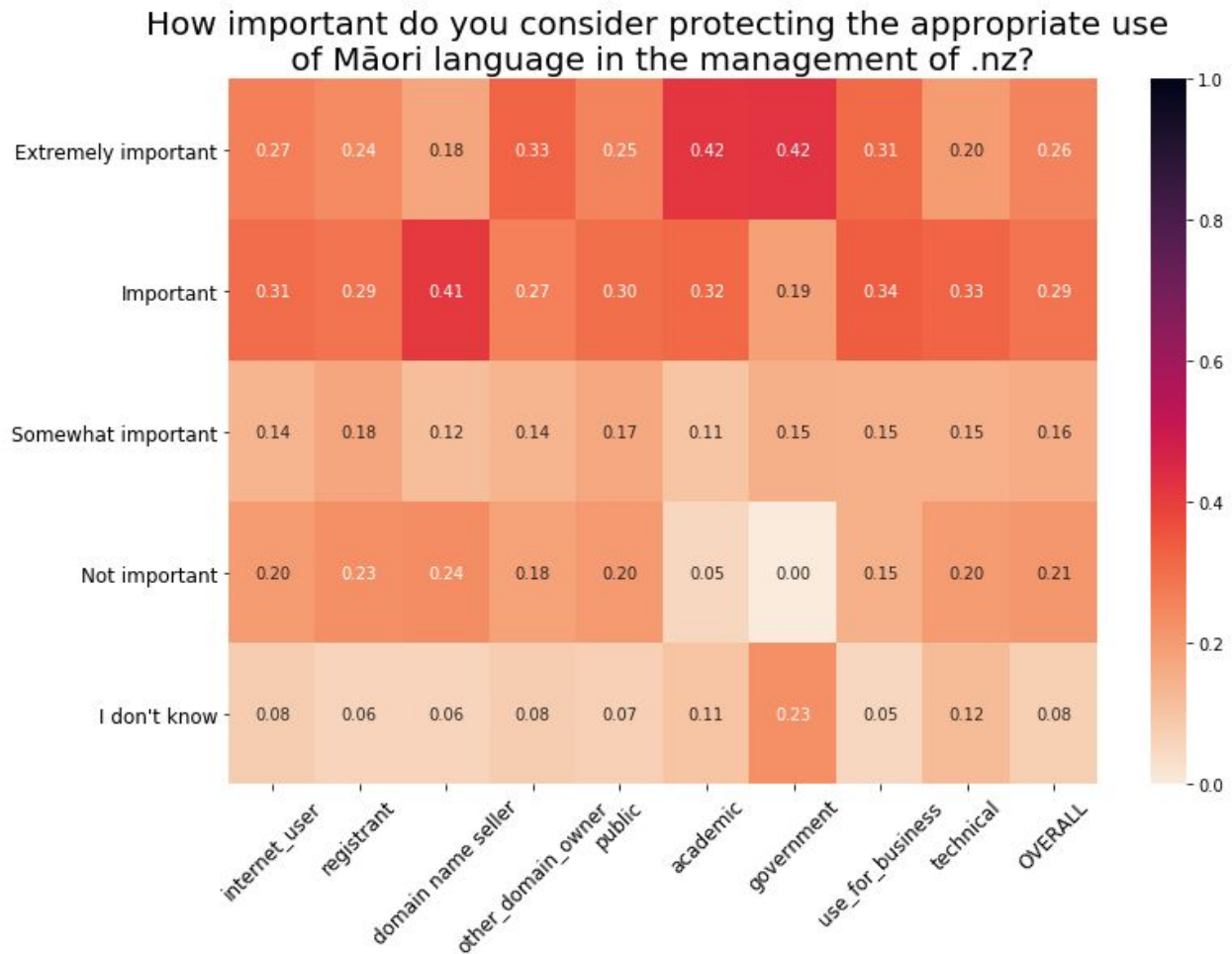
9. While respondents had varying views, overall there seems to be an understanding of the value of privacy for individuals, and accountability for organisations. Responses suggest that the IRPO is a good mechanism, if used correctly.
10. One respondent offers a detailed solution (paraphrased below):

The availability of information on domain name registrants needs to balance between the need for others to know "who is behind that domain name" (such as is possible with any trademark, company, etc), and the privacy/security of the registrant. The balance is that the: (a) name, and (b) general location (city, state, country) be easily publicly available, and some form of contact is available to the general public through additional steps, but that additional information (such as detailed physical location) be reserved for their registrar, the registry, and law enforcement. Businesses should have the option to publish their physical address, to bolster their credibility / provide a way to further determine who is behind that domain name.

Te Tiriti and Te Reo Māori

How important do you consider protecting the appropriate use of Māori language in the management of .nz?

Figure 12: Distribution of answers per respondent type for question 'how important do you consider protecting the appropriate use of Māori language in the management of .nz?'



Key findings

Academic and government respondents were the most likely to consider protecting the use of te reo Māori to be “extremely important” (42%). 21% of respondents consider protection of te reo Māori to be ‘not important’ in the management of .nz. Registrants and domain name sellers are more likely to hold this view, with 23% and 24% of respondents answering “not important” respectively.

Open ended response: protecting the appropriate use of Māori language in the management of .nz

51 respondents answered the open ended question “How important do you consider protecting the appropriate use of Māori language in the management of .nz?”

Some respondents want to see te reo Māori respected and promoted in the management of .nz

1. In the open ended responses, those who see te reo Māori as important mentioned various reasons:
 - a. 2 respondents mentioned that te reo Māori is an official language
 - b. 8 respondents noted New Zealanders have a responsibility under Te Tiriti to protect te reo Māori

Across questions of Te Tiriti and te reo Māori, some respondents want to see Māori views prioritised

2. Some respondents (9) replied to the open ended question about Te Tiriti by saying that we should defer to Māori. The same sentiment came up in the reo Māori section.
3. One respondent said *“Language means different things to different people. In the case of Maori language I understand it is integral with Maori culture, and as such we should defer to the guardians of that culture. In today's world it is not good enough to simply appropriate such things as though we were still operating with a colonial frame of mind.”*

Some respondents want to see better support for macrons (which .nz already supports)

4. Some respondents (6) want to see macrons supported in .nz domain names. Macrons are already supported, so there may be a lack of awareness about this support amongst potential registrants.

Some respondents do not see why te reo Māori should be protected over other languages

5. Approximately 22 respondents do not think that te reo Māori should be protected through the management of .nz.
6. 2 respondents offered the view that te reo could only be protected through the restriction of speech: *“There is essentially unlimited space for the*

expression of culture as things stand - would mandating particular representation drive people away from a domain and impose barriers to use?"

How should the management of .nz appropriately reflect the partnership intended by the principles of Te Tiriti o Waitangi/Treaty of Waitangi?

161 respondents answered the question asking how management of .nz should appropriately reflect the partnership intended by the principles of Te Tiriti o Waitangi/Treaty of Waitangi.⁶

Some respondents think Te Tiriti should not be considered in the management of .nz

1. 43 respondents think Te Tiriti should not be considered in the management of .nz.
2. 9 respondents think that all people should be treated equally in the management of .nz with no 'special treatment' for Māori or Te Tiriti.

Some respondents want to see greater involvement from Māori in the management of .nz

3. 10 respondents stated that .nz should adhere to the principles of Te Tiriti. 22 respondents want to see consultation with Māori, or a reimagined governance structure that embeds a Māori perspective for the management of .nz.
4. Some respondents offered ideas about how to include Te Ao Māori in the management of .nz:
 - a. *"Iwi should have have equal ownership of .nz, including determining management and governance processes, even where this means a substantial change to current practice."*
 - b. *"Iwi consultation (in region the .nz management is conducted), living wage, thoughtful hiring practises, emphasis on bilingualism/Te Reo."*
 - c. *"We need a wananga for this seriously, then at least we can inform the other IT roopu who operate in NZ that we have tikanga and tangata considerations. Heio ano, he hui tahi tatau please"*

⁶ 34 of these responses were variations of "I don't know" and we have omitted these from our analysis.

- d. *“fund work on data sovereignty, data trusts, Te reo on line, hand over half the cash to Maori - hard to do with no strings though (whanau ora of the Internet?)”*

The principles of Te Tiriti could be embedded in our approach to privacy, data protection, intellectual property and responses to abuse

5. Some respondents made suggestions about ways Te Tiriti should be embedded in .nz policies:
 - a. *“In general we're doing too little to reflect the principles of Te Tiriti o Waitangi in NZ. Any organisation visibly taking a lead role will progress our country in the right direction.”*
 - b. *“The privacy and protection of all users will include respect to Te Tiriti.”*
7. *“[we can reflect the principles by] monitoring of inappropriate use of Maori language, taonga, symbols.”*

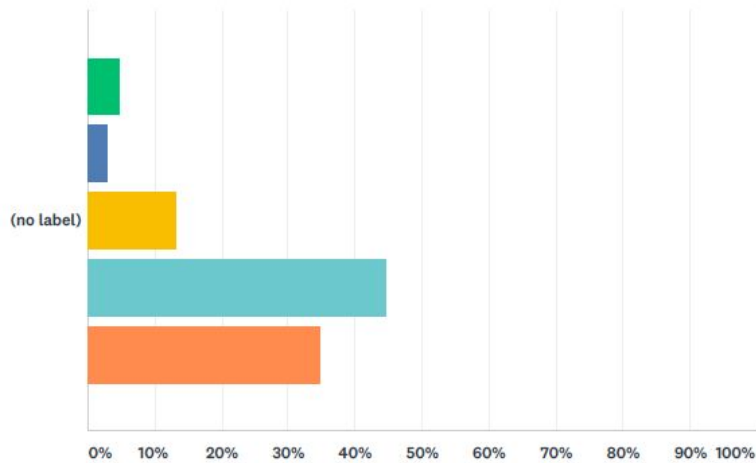
Human Rights

The chart below shows sentiment across all respondents on the importance of human rights in the context of the .nz policy review.

Figure 13: Distribution of answers for question ‘how important do you consider human rights (such as freedom of expression) are in the context of the .nz policy review?’

Q14 How important do you consider human rights (such as freedom of expression) are in the context of the .nz policy review?

Answered: 274 Skipped: 2



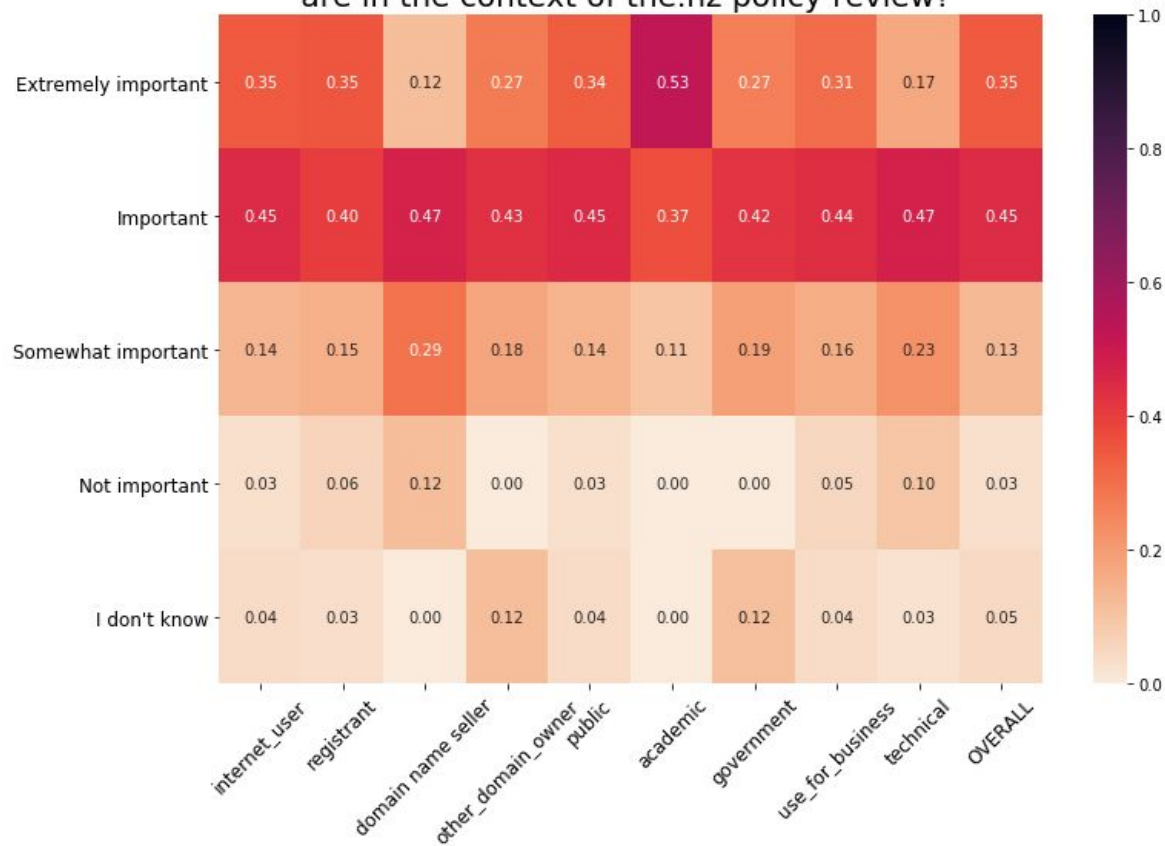
■ I don't know
 ■ Not important
 ■ Somewhat important
 ■ Important
 ■ Extremely important

	I DON'T KNOW	NOT IMPORTANT	SOMEWHAT IMPORTANT	IMPORTANT	EXTREMELY IMPORTANT	TOTAL	WEIGHTED AVERAGE
(no label)	4.74% 13	2.92% 8	13.14% 36	44.53% 122	34.67% 95	274	4.01

The next diagram shows how each type of respondent considered the importance of human rights in the context of the .nz policy review.

Figure 14: Distribution of answers per respondent type for question 'how important do you consider human rights (such as freedom of expression) are in the context of the .nz policy review?'

How important do you consider human rights (such as freedom of expression) are in the context of the .nz policy review?



Key findings:

1. Overwhelmingly, the majority (about 80%) of respondents thought human rights were “important” (44.5%) or “extremely important” (35%) in the context of the .nz policy review. Domain name sellers and technical respondents were less likely than other groups to consider human rights as “extremely important”.

Open ended question on human rights

There were 80 responses out of 276 to this open ended question. The key insights are summarised below:

New Zealanders are divided on how to approach free expression

2. Submitters diverge on how human rights should be applied. Of 80 open-ended responses:
 - a. about 11 think free expression should be protected at all costs
 - b. about 35 consider free expression should be protected but not if harm will occur (hate speech and violence)
3. Most respondents believe free expression is not absolute, and hate speech cannot be permitted (at least 45 respondents specifically say they think human rights are important, with an exception for hate speech). However it was unclear how they see this applying to .nz policies.
4. One .nz registrant said, *"It does need a finely tuned balancing act. Too much freedom of expression may be a catalyst for social bullying and further marginalisation of minority groups. Too little freedom of expression can lead to a harsh and repressive totalitarian society. Neither of these end results are desirable in Aotearoa."*

Some respondents do not see InternetNZ having a role in realising or promoting human rights online...

5. A few respondents expressed a desire for InternetNZ to operate a neutral DNS registry that did not make decisions about content. They viewed human rights as 'irrelevant' to the review.
6. From a technical sector person: *"Your role is managing and running DNS servers. That's where it ends. You map a domain to an IP address, everything else should be left up to the NZ legal system to deal with. Your job is not to decide what is 'good' and what is 'bad'. That is a legal issue, not something to be done by an NGO."*

...and others think InternetNZ should hold and enforce a strong opposition to hate

7. A few respondents suggested that regardless of human rights, InternetNZ should adopt policies that protect vulnerable Internet users and not allow hate on its platform.
8. From one Internet user: *"Although freedom of expression and hate speech can be bandied around (by those using hate speech typically) that they are allowed their freedom of expression, .nz should take a stand that they will not allow hate speech, radicalisation or extremist tendencies of any kind."*

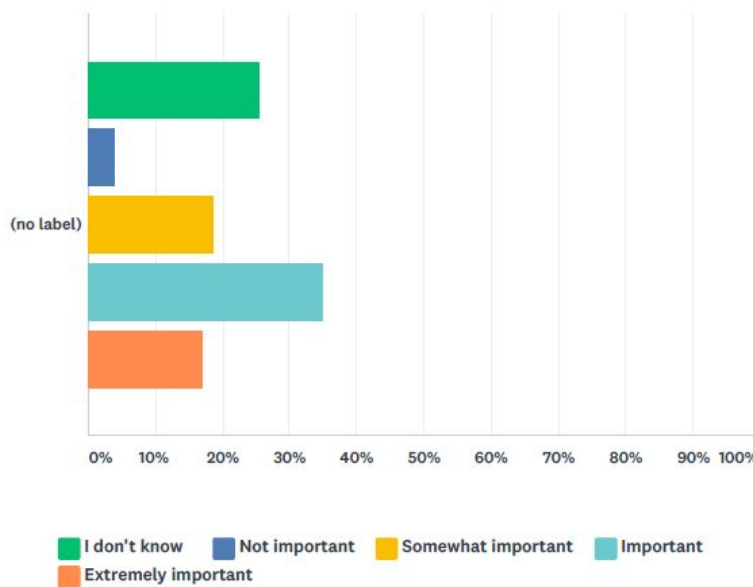
Business

The chart below (Figure 15) shows sentiment across all respondents on the criticality of .nz to NZ businesses.

Figure 15: Distribution of answers for question 'how critical do you consider .nz policies are in supporting or hindering NZ businesses to flourish?'

Q15 How critical do you consider .nz policies are in supporting/hindering NZ businesses to flourish?

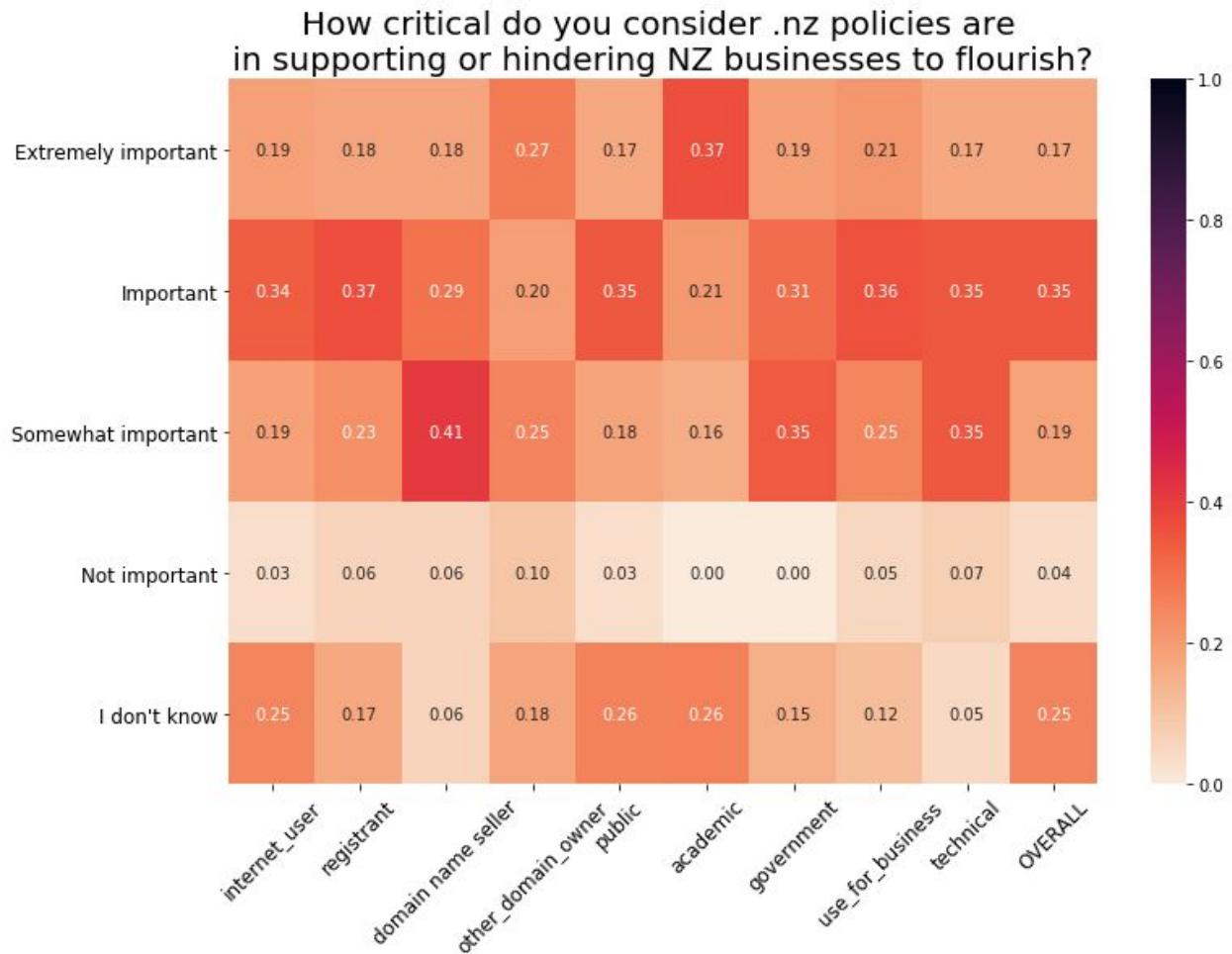
Answered: 275 Skipped: 1



	I DON'T KNOW	NOT IMPORTANT	SOMEWHAT IMPORTANT	IMPORTANT	EXTREMELY IMPORTANT	TOTAL	WEIGHTED AVERAGE
(no label)	25.45%	4.00%	18.55%	34.91%	17.09%	275	3.14
	70	11	51	96	47		

The next diagram shows how each type of respondent considered the criticality of .nz to NZ businesses.

Figure 16: Distribution of answers per respondent type for question 'how critical do you consider .nz policies are in supporting or hindering NZ businesses to flourish?'



Key findings:

1. Only 4% of respondents considered the policies are “not important” to supporting/hindering New Zealand businesses to flourish, including some (4 of 11) who are .nz registrants. A majority of respondents (35%) considered .nz policies are “important” to supporting/hindering New Zealand businesses to flourish with a fair amount (17%) considering the policies are “extremely important”
2. 41% of domain name sellers considered the .nz policies are only “somewhat important”. As these are people who are closely involved in helping New

Zealand businesses with their web presence, one can assume they may be better informed and have other insights into what businesses need to flourish.

Open-ended question on supporting New Zealand businesses

Only 29 of 271 respondents answered the open-ended question about supporting New Zealand businesses, and their perspectives were diverse.

Some respondents thought .nz limited a businesses brand to New Zealand

1. Some respondents had a view that if you wanted to be seen as a global business, you needed a gTLD like .com.
2. From a technical person who holds both .nz and non - .nz domain names: *“.nz needs to be trusted. But .nz mainly only carries value in NZ. If you're aiming overseas .nz is so small you want a .com”*

Many respondents stated that there were more important priorities than supporting business

3. Respondents used the open entry field for this question to talk about issues they see as more important than supporting businesses to flourish:
 - a. **Consumer protection:** *“It's not the domain's role to make NZ businesses flourish -- that's what business leaders are for. I'd like to see an emphasis on making policies that support NZ consumers.”*
 - b. **Human rights:** *“Provided it does not attempt to suppress or demean the rights of others.”*
 - c. **Trust in .nz:** *“People in NZ trust .nz domains more than others so it is important to keep that trust factor high.”*
 - d. **Security:** *“More and more companies are looking at online retailing, so it's of utmost importance to get security awareness across .nz businesses. If online e-commerce solutions keep getting bad publicity and press due to hacking or security concerns, it would lose credibility in the local market space with consumers. Just from an online payment point of view, some companies store credit card details that should not be doing so.”*

There are opportunities for .nz to help more businesses

4. One participant suggested that .nz should partner with the New Zealand Business Number (NZBN), to make it easier for businesses to be online: *“Make it easy for every business to have a website (with .nz domain). Also liaise with NZ Business Number to make this easier or cheaper but still secure”*.

What else respondents would like us to know

Respondents had an opportunity for additional input on .nz policies. Below are some of the unique insights expressed by individual respondents from this section.

1. Enable more domain name registrars to enter the market:

“InternetNZ should encourage more domain registrars/resellers. There are a few local registrars who continue to purchase all smaller registrars and dictate the market price to a certain degree. It should be easier for companies to become NZ domain registrars.”

2. Prioritise the wellbeing and safety of Internet users:

“The questions so far seem concerned with ensuring predatory online behaviour is not unduly shut down. If offensive speech or speech inciting hatred is protected as freedom of expression; or if dodgy business practices are protected in the name of 'supporting economic growth', then in my view you're headed down the wrong path.”

3. Monitoring and making decisions about content is a big change that must be considered carefully:

“You had best be careful about attempting content control, or you will become _responsible_ for content, which is largely out of your control! Stay neutral, and do your job. Even things like shutting down a domain should only be done with an order from law enforcement, not just because a staff member at InternetNZ or someone on Twitter disagrees or finds something offensive.”

4. If we get this right, we can improve the experience of the Internet for New Zealanders:

“You've got a big task ahead of you, balancing NZ's need for security and personal safety with commercial requirements and the 'freedom of speech' of haters. Good luck with finding this balance and starting a little revolution that begins with .nz domains and leads to bigger changes.”