Overview of submissions

This summary of submissions was produced to assist the .nz Advisory Panel with its consideration of submissions on *Re-imagining the future of .nz: Option Report of the .nz Advisory Panel.*

The consultation process

The .nz Policy Advisory Panel released *Re-imagining the future of .nz: Options Report of the .nz Policy Review* on Friday 17 July. This paper followed the Issues Paper released in February 2020.[1] The Options Report canvassed options on 23 issues identified by the Panel in their preliminary research and engagement with New Zealanders.

In addition to options for responding to the issues, the Report also included a set of new 'guiding principles' for the .nz domain name space and questions about how InternetNZ should engage with Māori on any further work on issues affecting Māori.

Consultation ran from 17 July 2020 to 14 August 2020, with extensions of up to two weeks for those who sought them. In addition to receiving formal submissions, the Panel also ran online webinars, and produced plain English accessible video and written content for New Zealanders to engage with.

Submissions received

During the consultation period:

- Held two webinars for the public, engaging with over 20 participants
- Received 13 submissions from individuals on the consultation paper
- Received 13 submissions from organisations and government agencies on the consultation paper
- Received 40 submissions on single issues from New Zealanders engaging with online content.

[1] https://internetnz.nz/assets/Archives/dotNZ-issues-report.pdf

For a full list of submissions to date, see the InternetNZ website: https://internetnz.nz/nz-domains/nz-policies/nz-policy-review/nz-have-your-say/

Comments on video and written content

As we wanted to reach everyday New Zealanders, we created easy to understand content covering a few issues that represented some of the big themes of the .nz Options Report. We promoted these through InternetNZ's channels and advertised on social media. As mentioned above, we received 40 submissions on this content.

How to read this paper

This document provides an overview of the feedback received by the .nz Advisory Panel on the Options Paper. It summarises the feedback on each issue and captures broad themes from the submissions. We have also provided Panel members with the full text of each submission.

We asked submitters to answer the questions that were most relevant to them, so some issues have more substantial feedback on them than others.

Submitters' comments are summarised against each issue. We have sorted them by their preferred option (ie, we have put those who preferred option A together, option B together etc).

Where option preferences have brackets around them, the submitter has not indicated a preferred option, but their comments reveal an inferred preference. Where submission feedback has content in square brackets this indicates where the meaning was not clear.

Some submitters may have made a comment but not indicated a preference, or vice versa. Where this is the case we have left the preferred option or comment field blank.

Feedback has been summarised, to help the Panel see the breadth of views on each issue.

Contents

Emerging themes

Below is a snapshot of some takeaways from the submissions we have received. We have identified themes, areas of contention and new ideas from submitters.

A guiding vision for .nz - who is it for, and how should it be run?

Submitters are generally supportive of a move to visionary, holistic, inclusive and instructive guiding principles

- Most submitters support the proposal to create a set of guiding principles and move some existing principles to be operational guidelines.
- Many submitters support the new principles as proposed, although there are some concerns for how the principles would impact .nz. For instance, some were concerned with how the 'New Zealand benefit' principle would be applied and measured. There were also strong views on how changing 'no concern for use' might impact .nz and the roles of InternetNZ and DNCL.
- A few submitters said that the principles needed to be worded carefully to reflect outcomes that are within the scope of .nz policies. For instance, one submitter commented that the 'open and accessible' principle "needs to be phrased in the passive sense of what the namespace will not prevent rather than the active sense of what it will aim to deliver".

.nz should reflect the diversity of New Zealand

- Many submitters support making the .nz policies available in more languages, and making more character sets available, so that the .nz domain name space is inclusive and reflective of a multicultural society.

.nz should be for New Zealanders

- Many submitters support restricting .nz domain name registration to people and organisations with a New Zealand presence only. Of the people who submitted on the web video about local presence requirements, 20 out of 21 people want to see .nz be for New Zealanders only.

- One submitter suggests an opt in local verification process instead of a local presence requirement:

> ”Additional information could be collected via the Registrar such as NZBN, verified contact details, RealMe identity verification, drivers' licenses etc and processed via API. A centrally operated website would allow internet users to enter a website address and verify its status, and the website operation to display a dynamic .nz trust seal on their website providing an additional level of trust for .nz.”

.nz should be accessible for people with disabilities

- A number of submitters note that, in addition to increasing accessibility by providing the policies in multiple languages, wider web accessibility should also be considered, including for people with disabilities.

Submitters support the proposal of a principle to support the use of te reo Māori and participation of Māori in .nz

- All submitters who responded to questions related to the proposed principle on te reo Māori and the participation of Māori in .nz support having such a provision. Some submitters were not sure about the wording of the submission, what it would mean in practice and whether Māori were involved in the drafting of it.
- All submitters consider that InternetNZ should engage with Māori when amending .nz policies and ensure it has adequate capability to facilitate engagement with Māori. One submitter suggested that work re-writing policies be paused until InternetNZ had engaged with Māori. Another submitter considered it important for InternetNZ, as a surrogate for NZ society, to meet Treaty of Waitangi obligations.

Submitters support retaining the Registry/registrar model

- All submitters support the retention of principles of “structural separation”, and “clear chain of relationships” that describe the model of separation between the Registry and registrars.

Security, privacy and trust - important issues with many answers

Many submitters agree with the Panel's assessment of issues on security, privacy and harmful uses of domain names in the Options paper. However, there is a lot of disagreement about how to respond to these issues and what InternetNZ's role should be.

Submitters recognize that security threats and harmful uses of domain names need to be mitigated...

- On the issue of the 'interim emergency clause', a majority submitters either support introducing a modified clause after feedback with the community, or they want to see the clause lapse but replaced with a more robust notifier scheme or acceptable use policy. All submitters supported some form of intervention on harmful content.
- Submitters acknowledge that the nature of online harms requires different responses and tools than offline harms:

> "An unfortunate characteristic of the Internet is that people who commit harm using the Internet can hide their tracks very well and the normal policing methods to detect, prevent and prosecute crime are struggling to be effective in this environment. In particular those methods operate at a very different speed to the Internet, where something like a phishing site can inflict considerable harm in just one hour.
>
> Consequently, the greatest disruption to criminal behaviour on the Internet comes from the actions of industry participants such as registries and registrars, who are able to act significantly faster than law enforcement. From a principled perspective this is not a position I want to see continue, but it is the reality on the ground and will be for many years to come and so should be accepted and worked within rather than rejected."

...but some submitters disagree on how best to mitigate security threats and harmful uses of domain names

- Submitters are split on whether to introduce security standards for registrars, largely for technical reasons.
- Some submitters support introducing a reserved and restricted names list. Others highlighted the difficulty of implementing a technical solution to offensive or misleading words:

> “An automatic scanning of names for strings would lead to absurd situations like the banning of shitakemushrooms.com. See https://en.wikipedia.org/wiki/Scunthorpe_problem.”

- Some submitters note the difficulty and and cost of proposed solutions. For instance on data validation:

> “Any attempt to verify or validate contact information is going to increase costs and be difficult to implement across all Registrars. Take for instance, verifying that a physical address exists. [...] There can be many inconsistencies with address data provided by various organisations, especially businesses.”

Many submitters are also concerned with scope creep and do not want to see InternetNZ or DNCL making decisions about responding to harmful uses of domain names

- A number of submitters want to see InternetNZ to focus on service delivery, but were open to relationships with enforcement agencies:

> “A far better approach would be to retain the “no concern for use” model, but partner with enforcement agencies and other industry bodies. Work closely with them and establish bi-directional communications.
>
> The banks don’t just freeze accounts as they please. NZ Post don’t confiscate parcels themselves. Storage providers don’t just turf people’s gear out. All these organisations work with government organisations and law enforcement agencies, such as Customs, MPI, NZ Police, the SIS, the GCSB, InterPol and the DIA. They maintain communication channels with these authorities, and refer matters to them for investigations to take place and/or action to be taken. It is only on instruction from those authorities that any revoking/cancelling/freezing take place.”

- Some submitters also raised freedom of expression concerns:

> “Tasking DNCL with having to take action against domain names being used legally but allegedly ‘inappropriately’, would potentially have a chilling effect on freedom of expression, not to mention the impossibility of deciding what is ‘inappropriate’ particularly as such values in society continually change.”

Submitters support a privacy-enhancing approach to registrant information

- Many submitters support protecting registrants’ data, by either collecting less personally identifiable information (PII), expanding the IRPO to be applied by default, or making it opt out.

> “Given the options to choose, cannot see why any individual would want their personal details, including email address, made publicly available.”

- Submitters do not support creating separate registrant types, due to technical complexity or the burden of validating the registrant types.
- Some submitters have recommended looking to the principles of the Privacy Act to inform the policy around collection and protection of registrant data

New ideas for technology specific language

- A number of submitters have suggested technologically specific guidelines outside of the principles which can be more easily updated than the core policies.

Enhancing .nz growth and improving market operation

Submitters support the existing market model

- As above, all submitters support the current principles of separation, and a chain of relationships between the Registry, registrars and registrants. On other issues related to registrars there were mixed views.
- Submitters had mixed views on how to respond to identified issues around how domain name players interact, and mostly did not support a change to how resellers are regulated.

Submitters support ending the conflicted names process

- Most submitters agree that the conflicted names process should end but there were mixed views on how to resolve the outstanding conflicts.

There are proposals for new second level domain names

- One submitter has petitioned for a new 2LD to be created: edu.nz.

- A few submitters saw the value in moderated 2LDs for specific high risk sectors, like banks.

Guiding Principles

1. Do you consider that the .nz guiding principles should be visionary, holistic, inclusive and instructive rather than operational?

Submitter		Summary of submission
Anna Pendergrast	Yes	Supports principles being visionary, inclusive and instructive. However, risk with “high level” principles that they are too vague to be useful. Needs to be really clear what these will mean in practice – what it actually looks like to be guided by these principles. Often principles just sit there and are not actually implemented in any meaningful way, despite best intentions. Having concrete clauses and technical, supporting operational guidance about what each principle looks like in practice could help mitigate the risk that the principles will not be used appropriately. In terms of holistic, the principles need to be accessible and understood by everyone in New Zealand but should speak specifically to people who will be required to make these principles a reality.
Anonymous - prior work in domain names	Yes	Supports guiding principles being visionary, holistic, inclusive and instructive.
Dreamscape Networks	Yes	Supports principles being visionary, holistic, inclusive and instructive. Existing .nz guiding principles capture part (but not all) of the key principles covering the various levels of domain name management. Not transparent. Supports the visionary component as vision and forward thinking has been lacking broadly across the domain landscape in the past. Instructive, and by association guiding, is key to encapsulate all the principles and create a journey which stakeholders can travel to drive the deeper understandings required respective to their position.
Jacinta O'Reilly	Yes	Supports .nz guiding principles being visionary, holistic, inclusive and instructive. .nz domains hold a special place for NZ. Anyone seeing the .nz in a name immediately knows the content has a NZ association. Perception even if not true. No company should have control of this domain

		unless they take that responsibility seriously. To have a policy of abdication of responsibility for the content of websites identified as with New Zealand is irresponsible. Administration of .nz domains should not be in the charge of those who do not consider good curation of content their responsibility. The people who wish to act in the interests of internet users who promote harmful and malicious content should not have access to .nz domains, as they bring the whole country into disrepute. A policy that allows the flouting of a flagship national initiative like “The Christchurch Call” could not possibly be acceptable to the governance of NZ. Interest of all New Zealand in preserving a reputation and a reality of commitment to the safety of all our people should be considered in this review.
Jannat Maqbool	Yes	Supports guiding principles being visionary, holistic, inclusive and instructive. Operational principles are more about the how rather than guiding the what and why. With the ‘how’ being more time bound in some cases. We want principles that are sustainable.
Jay Daley	Yes	Supports guiding principles being visionary, holistic, inclusive and instructive.
Keitha Booth	Yes	Supports creating visionary and aspirational principles which endorse an open and free internet for all and which do not include operational elements. The draft principles extend and explain clearly the vision for .nz but do not set out adequately the public good importance of a technically robust infrastructure openly available for all. InternetNZ has fiercely worked for, endorsed and delivered this in NZ since its inception. Draft principles deliberately scope and promote .nz to make it attractive to New Zealanders but equally important they are positioned globally and spell out technology principles. Should replace 'should' in each principle statement with 'must'. 'Must' indicates a fundamental requirement whereas 'should' suggests only nice to have.
1st Domains	Yes	Supports principles being visionary, holistic, inclusive and instructive. Changing to a guiding set of principles like those proposed will foster innovative approaches and flexible solutions to any challenges and changes the space may face in the future.
MarkMonitor	Yes	Has no objections to these principles.
Commerce Commission	Yes	Broadly supports the introduction of updated guiding principles.
OFLC	Yes	Supports principles being visionary, holistic, inclusive and instructive. Fairly significant change for the overarching principles to guide management of .nz. Submitter very supportive of it. Supports

		guiding principles being expanded. Reflects the way the digital space and use of .nz has changed over time. InternetNZ and the DNCL have a clear responsibility and role to play in mitigating harms in this area. New principles far more accurately show that. Would send a clear message to those who may be wanting to misuse .nz. General comment on new principles – they currently read '.nz should…'. Perhaps as guiding principles would be better to be frame them as '.nz is…' or '.nz aspires to be…' to capture the aspirational nature of them.
David Farrar		Possibly but not necessarily. Need to be careful with setting them too holistic. A guiding principle of "secure, trusted and safe" could be used to justify almost anything at all. No one wants to be against safety but safety can be used to justify arbitrary cancellation of domains that someone believes makes them feel unsafe. A guiding principle should be specific enough that people understand what the implications of adopting it mean, and be debatable in terms of pros and cons of including it.
Ben Bradshaw		Does not see any issue with having a mix of both, no need to throw away good existing principles just to bring in new ones.
Arran Hunt		Page 19 of Options Report mentions guiding principles being difficult to understand "unless you are an industry insider". Solution provided appears to change them from being rules to something else, and that this would make them more enduring. I disagree. If a rule is difficult to understand then you redraft the rule in clearer language. Removing the rule and replacing it with a less defined holistic approach moves situations from objective to subjective. Would be detrimental to InternetNZ members as it removes certainty, fundamental in any contract (which is what people are entering in to when registering a domain). Holistic approach to the application of what were principles is seen in several other locations through the Options Report. Easy to write "be holistic" but application is difficult. Extremely subjective and never clear to the InternetNZ registrants. Typically lawyers would be looking at how a judge applied that holistic approach, requiring the judge to provide a test to turn that holistic view into something more objective, and the factors to be considered. Has not seen any such tests or guidance in the report. Would recommend that, should a holistic approach be taken, it be as clearly defined as possible for the benefit of registrants and the NZ public.

DNCL		The principles are key to how .nz operates and should be instructive. Being an ‘operational’ guideline implies that it is optional, which it is most certainly should not be. Aside from that, it is important that the principles are created clearly with the interest of the public in mind. For the purpose of transparency, it is important that the definitions are clarified.
MEGA	No	Does not believe that the .nz guiding principles should be visionary, holistic, inclusive and instructive rather than operational. The established operationally focused principles provide a reliable level of certainty and clarity in a very technical area. Providing for principles of a non-operational nature, to which the operational provisions would then become subordinate, would sacrifice some certainty and clarity. Most obviously seen in trying to determine the degree to which the operational provisions would have to be bent in their application to meet the interpretation (which would involve a large degree of subjectivity) of ‘visionary, holistic, inclusive and instructive’ principles.

2. Do you think the .nz policies should be rewritten and simplified?

Submitter		Summary of submission
Anna Pendergrast	Yes	Supports rewriting and simplifying principles. Generally happy with the proposed principles.
Anonymous - prior work in domain names	Yes	No objection to rewriting and simplifying in principle. Depends on what the new policies are.
Dreamscape Networks	Yes	Supports rewriting and simplifying principles. Historically and broadly across other spaces the focus has been more around the legalities, indemnity and protections in place to achieve the goals and objectives of the space. Important but has resulted in a situation where they are difficult to consume for the average stakeholder, leading to poor understanding, poor perception and ultimately poor execution as the stakeholder has not understood their obligations.

Jacinta O'Reilly	Yes	Supports rewriting and simplifying principles. Will make them accessible. Impossible to be completely unambiguous but at least clear writing can provide a clear base for discussion.
Jannat Maqbool	Yes	Supports rewriting and simplifying primnciples. Will ensure they are accessible to all NZers.
1st Domains	Yes	Supports rewriting and simplifying principles. Should be combined into a single indexed document and be reviewed to minimise and simplify the language used. Does not consider the existing policies to be full of unnecessary jargon. Register, Registrar, Registrant, UDAI/EPP Code etc may sound technical to new domain holders, they are industry specific terms used world-wide and we should not invent new terms for the sake of simplicity.
MarkMonitor	Yes	Supports rewriting and simplifying principles. We are in agreement with the simplification of the policies where necessary in order to improve offerings, function and service provision.
DNCL	Yes	The policies should be rewritten with the interest of the public in mind. It is important that the reform keeps the following objective in mind: (1) retention of public trust; (2) protect DNS security and stability; and (3) sufficient support to maintain the ‘first come first served’ principle.
OFLC	Yes	Supports rewriting and simplifying principles. Rationale provided makes sense. Very supportive of any action taken that seeks to make information more accessible to enable people to make informed decisions. Options provided for simplifying the policy framework seem to be pragmatic and focused on getting the best outcome.
Ben Bradshaw		Consolidating disparate sets of policies has value, as does some simplified language choices. It would be a lower priority to my mind though.
Jay Daley	No	Does not support rewriting and simplifying principles. But should review against a new set of guidelines. Danger in simplifying the Operations and Procedures that registrants would be confused about the procedures they are required to follow, that registrars would offer an inconsistent interpretation of the policies and that DNCL would need to make arbitrary judgements on too many issues. Purpose of the .nz policies is not clearly understood and until that is pinned down the content and structure of the policies will reflect the style and preferences of the current set of authors. A set of guidelines for what the .nz policies aim to achieve should be drawn up and consulted on and the policies can then be reviewed against those. Those guidelines could include such elements as “ensure that registrars interpret the policies in a consistent fashion”. Issue with industry jargon has been overstated in the report. Terms that originate as technical acronyms often end up in common parlance or at least

		well-known within a specific product/industry. “Domain name” is a perfect example of this. .nz should not create its own industry jargon like IRPO. Only jargon that is common in the global industry context should be used.
MEGA	No	Does not believe the policies should be rewritten and simplified. Simplifying the policies risks losing certainty and clarity, which is needed in a technical field. Risk that consolidating documentation will not be any less confusing or intimidating for people outside industry. People interacting with the .nz policies already understand them and their application. Changing them would require the industry to reinterpret them, creating uncertainty. Does not agree that the existing principles are“difficult to properly understand unless you are an industry 'insider'”. Could simply add a glossary or deeper explanation of key terms and concepts where necessary. Not helpful to claim existing principles are not written in a sufficiently “inclusive and accessible way” when at the same time it is not clearly identified who the affected ‘stakeholders’ are and their priorities which the principles supposedly need to be rewritten to align with.
David Farrar		This is almost a trick question. No one wants to argue against simplified policies. But implicit assertion that the policies are not clear enough at present. Can simplify policies by having 15 different policies each with its own subject area (so you just find the one you need) or by having just one policy that has everything included (which means all in one place). Need to decide on the substance on the policies and then decide how best to present them.

3. Do you think there should be a new ‘secure, trusted and safe’ principle?

Submitter		Summary of submission
Anonymous - prior work in domain names	Yes	Supports new principle, except that losing “no concern for use” puts InternetNZ / DNCL in the situation of having to be a judge in areas outside its competencies. Would prefer a strengthening of relationships with suitably experienced external agencies to remove concerns around scam & hate speech.
CERT NZ	Yes	Agrees infrastructure should be secure. Agrees the .NZ user experience should also reflect this. NZers should be able to use .NZ domains safely & securely.
Dreamscape Networks	Yes	Supports new principle. Important that principles guide what to expect further down the journey whether that is relative to process, management, policy or anything else that may be exposed to the stakeholders. Formulation could be more visionary. Says what the domain space “should” become but does not quite hit hard enough about what it wants to become. Soft statement .
Hein Frauendorf	Yes	Supports new principle. From a “standard” Internet user’s point of view, any .nz domain should imply a certain level of trust and security.
Jacinta O'Reilly	Yes	Supports new principle. Owe it to users and providers to take responsibility for the impact of our action. The internet is a part of society now and is part of the fabric of society.
Jannat Maqbool	Yes	Supports new principle. Puts thinking around these concepts at the forefront so that security, trust and safety are included by design in the application leveraging the .nz domain develops. Also benefit to consumers of the content.
Jay Daley	Yes	Supports new principle. Very basic moral obligation. If InternetNZ is not willing to include this then it should reconsider if it is the best organisation to act as the steward of .nz.
1st Domains	Yes	Supports new principle. Focus on security, safety, and trust in the technology and online space has progressed since the original policies written. Now a completely different climate. Public has a higher expectation that tighter security standards, encryption, online identity-verification and other technologies are available and embraced to enhance the online trust environment.
MarkMonitor	Yes	Supports new principle.
Liverton Security	Yes	Supports new principle. InternetNZ and registrars have a responsibility to the New Zealand public to provide a service which is secure, trusted and safe.

Ben Bradshaw	Yes	Supports new principle. This should not be interpreted as support for removing 'no concern for use'.
Office of the Privacy Commissioner	Yes	Agrees the .nz domain should be secure and trusted. Considers the principle could significantly change InternetNZ's role and responsibilities. Change could mean InternetNZ becomes an arbitrator of activity within .nz domains. Keen to understand what this role would look like in practice and whether the Panel anticipates a change in the collection or use of personal information to fulfil this new function.
OFLC	Yes	Supports new principle. Adding a clear principled focus on security and safety is important and timely. Current guidelines are silent in this area, which is notable. Adding new principle in this area would be positive. May require assessment of whether the existing practice needs to be adjusted to realise this principle. Agrees it is time for InternetNZ to move away from a 'no concern for use' mindset. Environment has shifted so much that we need to be consciously aware of everyone's responsibilities in this space. Could be strengthened by splitting the principle into two separate principles (given this principle is focused on two areas). Could be done as follows: **Secure and Reliable** **.nz infrastructure is dependable, resilient and secure:** any users of .nz are assured that the infrastructure is secure, current and reliable, has good resiliency and provides security for its users **Trusted and Safe** **.nz is a place that is safe and trusted:** .nz is a domain that people trust and feel safe to use. .nz users know that their privacy is protected and are given other options Also supportives suggestion that InternetNZ provide options and support for when something makes people feel unsafe. Will be opportunities to connect to agencies like the submitter to assist with this and to direct people to.
Berend de Boer	No	Does not support new principle. Would lead to setting up an alternative justice system.
MEGA	No	Does not support the new principle. Supports the motivation behind the desire to have it but does not believe it is necessary or appropriate. The successful operation of a domain name system requires that it be secure and operationally robust by its very nature. No advantage in placing a 'principle' on top of what is already clearly an operational necessity. Already sufficient

		protection and recourse for people currently existing frameworks in terms of promoting a ‘trusted and safe’ domain name system. Privacy Act, the Harmful Digital Communications Act and the Films, Videos and Publications Classification Act already provide protection. Agencies like Police and Department of Internal Affairs provide protection too. DNCL attempting to oversee, regulate and assist these aspects of the domain name space risks wasting its resources by duplicating oversight provided by other well established and specialised mechanisms. Could also confuse people about whom they should contact if any issues arise. Concept of ‘secure, trusted and safe’ could easily be seen to encapsulate responsibility for combating and providing some form of defense against a number of specific threats present in the online environment today, like the proliferation of malware and identity theft. Shows the danger of adopting such open ended concepts as ‘ secure, trusted and safe’ into the principles. Result could place responsibility on DNCL to consider oversight of areas few would rationally have thought DNCL could have any obligation to respond to or regulate.
DNCL		The Options Paper suggests that the new principle would replace the current ‘no concern for use’. The DNCL does not support such move as it would alter the neutral role that the DNCL and InternetNZ has in facilitating the way the domain names are used. The DNCL should not take on the role of a content assessor. We are the enforcer of the .nz Policy, not an assessor of online content.
David Farrar		Wary of this principle because of where it may lead. Could use it to mandate use of DNSSEC or implement a censorship regime that deletes domains that make people feel unsafe. Trusted is good but secure and safe can mean vastly different things to different people. Queries evidence base on how .nz is currently seen whether there is a problem to be solved by principle.
Arran Hunt		Options Report states various times the use of a .nz domain will provide people with increased trust and reduced concerns about security or harm. Later, there are discussions on whether certain standards are required. In a highly divided and developing landscape, the setting of standards for security and safety is very difficult. Typically, if left too loose there is a false sense of security. It wound too tightly, there is an impediment to innovation as there is no room to move. Queries whether InternetNZ would be opening itself up to liability if it promoted a

		requirement for safety and security but it was not provided. Not sure how this would work without massive costs to InternetNZ and registrants, and without creating liability.

4. What would be the main benefits and disadvantages of moving from a ‘no concern for use’ principle approach to a ‘secure, trusted and safe’ principle approach?

Submitter	Summary of submission
Blacknight	Internet has matured. Now concerns for many are around security and safety. Reflecting this in a ccTLD’s approach makes sense.
CERT NZ	Quicker intervention leading to a better user experience. Also minimises financial and data loss, as well as enhancing our overall digital economy.
Dreamscape Networks	A bit misleading. Particularly in today's world there is plenty of concern for use. No notable disadvantages to this. A more inclusive approach is certainly more palatable.
Edwin Hermann	Move unnecessary. The more regulation implemented, the more difficult it would be to determine whether the balance is right and the more time would be needed to deal with nuanced issues arising from that. Attempting to police and resolve these issues will necessarily involve additional resources. Seems unwise and unnecessary. Would also involve duplication of effort. Existing law, practices and precedents already exist that deal with many issues related to moving away from “no concern for use”. E.g., if someone is hosting illegal material, already a legal framework and government agencies in place to identify, take action, and ultimately resolve the situation. Should not duplicate this. Would be re-inventing the wheel. No reason to do so. Addressing issues already covered by legislation or law enforcement agencies would likely introduce inconsistencies. E.g., two trade marks that legally coexist (and tested in court). Plausible that .nz rules would not allow the holder of one trademark to register it as a domain because it is too similar to the domain name held by the other trade mark holder. Would be incredibly frustrating for affected business and individuals. All agree that .nz better off without harmful use. However, introducing new rules and policies will give people a false sense of security. Moderated 2LDs provide people with security and assurance, and rightfully so. Can be certain that, for e.g., a .govt.nz website will be owned and operated by a bona

	fide government organisation and therefore will almost certainly not be a harmful site. But attempting to set rules around the use of .nz domains will be nowhere near watertight so (unlike the moderated domains) people will falsely assume that .nz is generally safe. Far better approach would be to retain the “no concern for use” model but partner with enforcement agencies and other industry bodies. Work closely with them and establish bi-directional communications. The banks do not just freeze accounts as they please. NZ Post does not confiscate parcels itself. Storage providers do not just turf people’s gear out. They all work with government organisations and law enforcement agencies like Customs, MPI, NZ Police, the SIS, the GCSB, InterPol and the DIA. They maintain communication channels with them and refer matters to them for investigation and action. It is only on instruction from those authorities that any revoking/cancelling/freezing happens. Should therefore retain “no concern for use” model and combine it with the establishment of a much closer working relationship and open lines of communication with relevant authorities. Better for everyone. Does not impinge on freedoms.
Frank March	These are good and successful examples of authorities with responsibility for some form of regulatory authority within an appropriate layer of Internet activity. Counter example is the censorship filters in the UK and Australia where clumsy intervention at the addressing layer in order to censor at the content layer has created unintended and inappropriate consequences. At least NZ content filter has a degree of expert oversight in its operation. Should resist involving the .nz manager in content regulation. Should only “take down” site or block an activity at the behest of an appropriately empowered legal authority.
Hein Frauendorf	Will benefit Internet users in general but even more so Kiwis. Having a namespace that we know had a level of scrutiny applied, with the ability to report and have malicious websites removed quickly and easily, will leave New Zealanders with a uniquely trusted service.
Jay Daley	People who commit harm using the Internet can hide their tracks very well. Unfortunate characteristic of the Internet. Normal policing methods to detect, prevent and prosecute crime struggle in this environment. Methods operate at a very different speed to the Internet, where something like a phishing site can inflict considerable harm in just one hour. Actions of registries, registrars and other industry participants provide the greatest disruption to criminal behaviour on the Internet. Can act significantly faster than law enforcement. Not ideal from a principled perspective but it is the reality will be for years to come. Should therefore accept and work within the situation rather than reject it. Criminals gravitate towards registrars and TLDs that turn a blind eye to their activities. .nz thankfully has a strong set of registrars who take this seriously. Population size also

	presents a relatively small target for criminals. Together those have kept crime and harm low compared to other TLDs. However, registry should not have policy settings that ignore the direct impact that a registry can have in mitigating harm either. E.g., a phishing site that uses TradeMe branding and site structure to steal user logins and has no other purpose (i.e., a domain name registered solely for criminal purposes not a compromised site or hijacked page). Current policy requires TradeMe to get an emergency court order to take the domain name. By that time thousands of user logins could have been compromised. Unconscionable as there is no ambiguity around criminal purpose. .nz should take that domain name down once validated. Significant risks if that power is misused or incorrectly used but many registrars and other registries have systems and safeguards. Can do the same.
1st Domains	Protecting the integrity of the .nz space with a proactive approach would become a priority in everything from policy to operations. There would likely be an increased level of overhead from monitoring and acting on any breaches.
MEGA	Does not support a move from a ‘no concern for use’ approach to a ‘secure, trusted and safe’ approach. Disadvantages set out in question 3 above.
MarkMonitor	More modern approach to dealing with current domain issues such as DNS abuse and abusive registrations. Shows the registry is taking a proactive approach to registrants and registrars.
DNCL	Benefits: More direct control of content and safety online Potential increase in trust in the .nz domain name space Disadvantages: The DNCL should not take on the role of a content assessor. We are the enforcer of the .nz Policy, not an assessor of online content
Ben Bradshaw	Does not see how adding things like DNSSEC and registrant privacy in any way conflict with ‘no concern for use’. Not in favour of removing ‘no concern for use’. DNCL are best positioned when they maintain neutrality and have to be an arbiter in such matters. They can also act as a check and balance on any order to restrict a domain name. Are times when it is best for the NZ public to restrict access to a domain name quickly, especially after a terrorist incident. Organisations like the OFLC can declare items to be restricted. As part of that, submitter prefers them to be able to identify and restrict domains rather than DNCL. After the Christchurch Mosque attacks the shooters ‘manifesto’ began circulating online. Was not just through domain names in the .nz space. Was through social

	media and file sharing tools as well. Removing content from web involves more than DNS controls. “They should also be able to trust that people they engage with online are who they say they are.” Does not believe DNS is part of the trust and identity verification process any customers or Nzers use to verify online identity, nor is it likely to be so.
OFLC	Key benefits in shifting approach in this context are: ● Sending a clear message to all stakeholders that the ‘care factor’ is increasing is positive ● Allowing InternetNZ better reflect the shift that they have already started to make in practice ● Setting an expectation for internal staff – which in turn should drive practice ● Adding value to overall eco-system in NZ ● Positive reputation – with particular groups in society (national and international) Possible disadvantages: ● Managing expectations – cannot make everything safe always, what does this mean in practice? ● Possible resource implications (if this is something that goes ahead and behaviour/process needs to change to implement) ● Negative reputation – with particular groups in society (national and international)
David Farrar	Disadvantage is once you start judging domain names by the use registrants make of them, you end up with an ever increasing censorship regime. In .uk the vast majority of domains deleted are around copyright complaints. Also greatly increase the legal risk to InternetNZ by taking on a subjective role in deciding whether use is of concern.

5. Do you think there should be a new ‘open and accessible’ principle?

Submitter		Summary of submission
Anonymous - prior work in domain names	Yes	Supports new principle. Thought we already had this. Perhaps it was unstated.
Blacknight	Yes	Supports new principle. In line with generally accepted concepts of inclusiveness and freedom to innovate.
Dreamscape Networks	Yes	Supports new principle. More visionary principle, particularly in contrast to the above. “Secure” and “safe” considerations could potentially be rolled into the content of this principal. However, would likely diminish the focus on security and safety within the space.
Hein Frauendorf	Yes	Supports new principle, with the exception of harmful content.
Jay Daley	Yes	Supports new principle but not as worded. “Inclusive” is generally taken to mean a safe space without hostile content or behaviour. That is not possible within a ccTLD namespace as that will reflect the wide variety of views of the whole population. Needs to be phrased in the passive sense of what the namespace will not prevent rather than the active sense of what it will aim to deliver.
1st Domains	Yes	Supports new principle. Important guiding principle to have, in conjunction with ‘secure, trusted and safe’ given that some approaches to improve trust and safety could directly reduce accessibility to the space by introducing restrictions and complexity
MEGA	Yes	Supports new principle as an addition to those currently existing guiding principles rather than as replacement for any currently existing guiding principles. Principle would support the ongoing innovation of the .nz domain and related services if instituted in a commercially prudent manner. However, this innovation and growth would be subject to the openness and accessibility not being achieved at the detriment of certainty and commercial effectiveness about how the domain name system runs. Test of not derogating from the certainty and commercial effectiveness of operation should always be a key assessment of any change

		proposed to the fundamental nature in which the domain name system runs.
DNCL	Yes	The DNCL supports a new ‘open and accessible’ principle. It is an important principle to have to achieve an open internet. Currently, the only registration restriction relates to moderated names and whether the domain name is already registered.
OFLC	Yes	Supports new principle.
David Farrar	Yes	Supports new principle.
Ben Bradshaw		Supports new principle. Not sure ‘innovate’ is needed as a word in the principle. It describes only one kind of potential use. Principle is to be open and accessible for any use.
MarkMonitor		No comment
Jannat Maqbool		Having this as a principle is likely to influence the application leveraging the domain being more open and accessible and then also potentially even the behaviour and thought processes of those leveraging the domain. [Is concerned about how registrants could exploit this principles]

6. Do you think there should be a new ‘New Zealand benefit’ principle?

Submitter		Summary of submission
Anna Pendergrast	Yes	Supports new principle but the proposed wording needs reconsidering. Not clear whether intended to be for the benefit of New Zealand as a whole (“NZ Inc” for lack of a better term) or just New Zealanders. Needs to be teased out a bit more. Not sure “New Zealander” is the right word – this speaks to people with citizenship and does not obviously include the many businesses and other entities within New Zealand. Could be broader to include “all people and organisations in New Zealand” or similar. Would however need to consider whether the domain should benefit the many ex-pat New Zealanders as well or more geographically about the country and people living here.
Jay Daley	Yes	Supports new principle if it is balanced against (1) global nature of the Internet where the actions of people on one side of the world can affect those on the other (2) need to ensure that .nz learns from international experience and follows international best practice rather than repeatedly reinventing the wheel.
Blacknight	Yes	Supports new principle. .nz namespace is clearly linked to NZ and reinforcing what was already inferred makes sense.
Hein Frauendorf	Yes	Supports new principle but even more-so to protect the public from harm.
Ben Bradshaw	Yes	Supports new principle. Well written as-is.
David Farrar	Yes	Supports new principle. Merely an extension of RFC 1591 which mandates a ccTLD should serve the Local Internet Community.
OFLC	Yes	Supports new principle. Supportives current draft formulation of the principle and the rationale to support it.
1st Domains	No	Does not support new principle. Aim of principle would be covered by the ‘open and accessible’ principle. The principle could even contradict being open and accessible, as it may

		be interpreted as being 'nationalistic' resulting in a restricted for NZ use only. Does not support that.
MEGA	No	Does not support new principle. Would allow actions and policies which could endanger the certainty and commercial effectiveness of operations of the .nz domain. Would also raise questions about how to view and treat the activities of businesses operating in and contributing to the NZ economy but that are part of larger global corporations or have significant or complete foreign ownership. Treating these businesses differently to other NZ business with less foreign composition could tarnish the reputation of the .nz domain overseas. Would hurt NZ businesses operating through a .nz domain internationally. Certainty and the commercial effectiveness of operations of the .nz domain is of prime importance. Should be an overarching consideration, regardless of the registrant business' nature, structure or ownership composition. However, depending on the wording of the principle and the way it was applied, may not oppose the establishment of one or more specific 2nd level domains under the .nz domain (e.g. something such as 'local.nz') which were the only domains under the .nz domain structure the principle was to apply to.
MarkMonitor		No objections
Anonymous - prior work in domain names		Not sure. Not clear who would be the judge of whether there was benefit to NZ.
Jannat Maqbool		[Is concerned about how registrants could exploit this principle]
Dreamscape Networks		Might be a bit polarising. Worthwhile containing content relative to the overall vision of NZ's approach to Digital Transformation. However, principle does depict a level of pigeon holing the space and does not speak to the significant ground that NZers have made through innovation and forward thinking that has taken them to the global stage.
Jeremy Johnson		Feels too easy for international businesses to capitalise on .co.nz domains. Has been an increase of international stores with long shipping times appearing to offer free NZ shipping

		trying to mislead NZ consumers. Also using nz.theirstore.com and theirstore.com/nz/ sub domains and URL structures do do this if they do not have the .co.nz domain.
DNCL		The DNCL finds the NZ benefit test to be too difficult to administer to support introducing the principle. No details of this test have been provided and the DNCL is not convinced that it is possible. We can take from the Overseas Investment Office's own 'for New Zealand benefit' test the difficulty to enforce such an objective test. It will also be difficult for the domain name to signal to users that it had gained the status of 'NZ benefit'.

7. Do you think there should be a new principle on te reo Māori and Māori participation in .nz?

Submitter		Summary of submission
Anna Pendergrast	Yes	Supports new principle, although would like to be sure that appropriate work alongside Māori has been done on the wording of it.
Blacknight	Yes	Supports new principle. .nz ccTLD should serve all the peoples of New Zealand, so it makes sense.
Dreamscape Networks	Yes	Supports new principle. Clearly important matter for all people of New Zealand. Calling this out and enabling it to drive the variety of initiatives in and related to the sector will result in good things.
Jay Daley	Yes	Supports new principle. This is obvious. However, does not support the principle as written because it is unclear what it means in practice. Could be an operational principle if it could be tightened up.
1st Domain	Yes	Supports new principle.
MarkMonitor	Yes	Support Māori participation in nz.
Ben Bradshaw	Yes	
OFLC	Yes	Supports new principle and draft formulation. Proposal would be strengthened through engagement with Iwi.
David Farrar		Supports principle around te reo Maori. Has some reservations around the participation principle. Not opposed to such participation, which would be absurd. Reservations because it is unclear what would and would not satisfy such a principle. Could argue allowing Māori to join InternetNZ is enough. Or could argue that to meet this principle there must be a parallel Māori body to InternetNZ that has veto over .nz policies.
Anonymous - prior work in		As a surrogate for New Zealand society, our Treaty obligations need to be met by the administration of .nz. Does not have sufficient knowledge in this area to input.

domain names		
Edwin Hermann		Should encourage the use of the Māori language and .nz systems and policies should facilitate this. However, policies should not come at the expense of freedoms elsewhere. Allowing the use of macrons is an example of an initiative that directly supports the use of Māori language and has no negative effects elsewhere. However, introducing a policy that said macrons were compulsory for domain names with Māori words (or the opposite: no macrons can be used unless it is part of a Māori word) would unnecessarily restrict freedoms (whether for Māori or non-Māori) and would do nothing per se to directly support the goal of facilitating the use of Māori language.
Jannat Maqbool		[Is concerned about how registrants could exploit this principle]
DNCL		The DNCL chooses to review the feedback from the community before deciding to comment on this question.

8. Do you think there should be a new guiding principle on enabling New Zealand to grow and develop?

Submitter		Summary of submission
Blacknight	Yes	Supports new principle. Reinforces the importance of digital.
Dreamscape Networks	Yes	Supports new principle. Most exciting of proposed principles. Speaks to the inclusive nature of driving growth and innovation. Far more valuable than the "NZ benefit" principle proposed.
Jay Daley	Yes	Supports new principle. Uses the word "enable" and "help" interchangeably. Quite different meanings. Supports "enable". Implication of a passive action in creating a namespace where growth and development are enabled. Does not support "help". Implication of taking specific actions to drive growth and development.
UniversitiesNZ	Yes	Supports new principle. Guiding principle on enabling New Zealand to grow and develop is an essential component of preserving and increasing the value, desirability and significance of the .nz namespace. Principle as suggested would be important to all organisations but particularly so those that face sector-wide challenges which could be addressed by changes to current policies or procedures relating to the .nz namespace.
OFLC	Yes	Supports new principle and draft formulation. Digital engagement and the procuring of .nz domains enables NZ business to take their services global. .nz should be seen as a part of their trusted brand.
David Farrar	Yes	Likes this principle
MEGA	No	Does not support principle. Similar to reasons outlined on question 6 above, certainty and commercial effectiveness of operations of the .nz domain is of primary importance. Principle seeking to place the interests of 'NZ' (however subjectively interpreted) above or alongside certainty and commercial effectiveness could pose a significant threat to the effective longer-term operational performance and reputational standing of the .nz domain.

1st Domains		Sounds nice but not sure how it can be achieved through providing domain names. Services built on top of the domain names help New Zealand grow and develop. Domain name is an enabler. May be possible to deliver on this principle with supplementary services where InternetNZ is in a unique position to offer other services drawing on its expertise and data for NZ benefit.
Jannat Maqbool		Submitter is not sure what this one means.
MarkMonitor		No Comment.
Anonymous - prior work in domain names		No opinion.
DNCL		[As per question 6] we can take from the Overseas Investment Office's own 'for New Zealand benefit' test the difficulty to enforce such an objective test. It will also be difficult for the domain name to signal to users that it had gained the status of 'NZ benefit'.

9. Do you think there should be two types of principles (guiding principles and operational guidelines to help manage the .nz domain? Why / why not?

Submitter		Summary of submission
Anna Pendergrast	Yes	Supports. But should be clear how the two interact. E.g. will there be one set of general operational guidelines or guidelines for each principle and what this means in practice. Needs to be clear link between the principles and operational guidelines.
Anonymous - prior work in domain names	Yes	Supports. If no operational guidelines the guiding principles will become large and unwieldy.
Dreamscape Networks	Yes	Broadly supports. Would be beneficial to have the guiding principles lead into the policy and process matters and not attempt to summarise or define them. Debatable whether the secondary component is considered to be the operational guidelines.
Jannat Maqbool	Yes	Supports. Operational principles are more about the how rather than guiding the what and why. The how is more time bound in some cases. Want principles that are sustainable.
Jay Daley	Yes	Supports, Useful distinction. Operational principles would presumably be subject to a more regular review and update than the guiding principles.
1st Domains	Yes	Supports. Makes sense. Guiding principles should not change but the operational guidelines could be regularly reviewed and altered to accommodate the changing environment.
MarkMonitor	Yes	Supports. Agrees with the notion of separating out the operational and functional guidelines from the principles of the Registry.
DNCL	Yes	Supports. Difference between ‘guiding’ and ‘operational’ (refer to Q 1). Considers there should be a policy meta policy or amendments to the PDP policy to govern policy terminology.
OFLC	Yes	Supports. It is important to have operational guidelines that can provide staff with clear guidance on how to realise the overarching guiding principles. Current guiding principles

		identified are important and would need to be retained operationally. Operational principles could be used internally – as part of operational policy for staff and the guiding principles be what is shared publicly. Important that any operating principles clearly connect to overarching guiding principles and that there is clear escalation and understanding of the guiding principles to resolve any issues.
David Farrar	No	Does not support. Unpersuaded that a hierarchy of principles is useful. If we want .nz to be simple we should have just one set of principles.
MEGA	No	Does not support. Should not be two types of principles (guiding principles and operational guidelines). Particularly not if the guiding principles would prevail if there is an inconsistency. Domain name space is a very technical area. Best option is the certainty of the current situation - the clearly operational matters in the existing guiding principles are not fettered by the subjective interpretation of new overarching less operationally focused principles.

10. Do you agree that the 'rule of law' principle should not be retained as an operational guideline?

Submitter	Summary of submission
1st Domains	**Supports removing the principle.** A given that NZ law applies.
Jay Daley	**Supports removing the principle.** It does not add anything to the default scenario.
OFLC	**Does not need to be an explicit principle.** Clear requirement as part of operating within NZ law – this does not need to be an explicit guideline. May be beneficial for international people to clarify somewhere that participants in the .nz domain must adhere to NZ law.
Blacknight	**Not sure** it needs to be explicitly included. No reason to exclude it either.
MarkMonitor	**Neither for nor against**. As long as the registry retains the ability to suspend domain names in exceptional circumstances (e.g. Covid).

Anonymous - prior work in domain names	**Does not understand the issue.** New Zealand law applies to the operation of the .nz domain name space. No foreign laws should ever be applied.
Dreamscape Networks	**Retain somewhere**. Important to maintain some reference to the application of laws and that the domain space is not entirely a free space. Could perhaps be more clearly encapsulated in the other operational principles as we agree its current form is not appropriate.
DNCL	**Does not support removing the principle.** While the principle might not apply in most situations, it serves as an indication of an overwhelming interest of justice to prevent situations where the Policy might lead to an unjust outcome. The goal continues to be to: ● improve observance with the law and the effectiveness of the regulator; ● deter misconduct and ● ensure that grave misconduct meets with proportionate consequences.
MEGA	**Does not support removing the principle.** Vital that we do not lose sight of the importance of the .nz domain space continuing to be operated in a certain and predictable manner. Certain legislation and agencies are relevant to the operation of the .nz domain. Therefore vital that the ‘rule of law’ principle be retained as a reminder that whatever other specific principles and operational guidelines are adopted moving forward, they all need to easily work in with and respect the basic philosophical tenets of the ‘rule of law’. Supports comments of the former Domain Name Commissioner quoted on page 27 of the Options Report that the ‘Rule of Law’ principle. Especially if principle removed, changes made to how compliance is adjudicated and enforced in the new operational matrix of the .nz domain should provide maximum allowance for due process at all times, including such standard features as prior notice, impartial hearing, right of appeal etc.
Jannat Maqbool	**Does not support removing the principle.**
Keitha Booth	**Does not support removing the principle.** High level principles covering the current rule of law principle should be retained.
David Farrar	**Does not support removing the principle.** Just because it is required is not the same as seeing value in emphasizing it. Having such a principle has helped guide InternetNZ into withstanding requests to ignore the rule of law and act upon accusations of wrongdoing.

Arran Hunt	**Does not support removing the principle.** Disagrees that principle does not provide meaningful guidance to participants in the domain name system. Knowing that the rule of law applies is in itself guidance. Helps make clear there are well-established and clear laws in place, unless it is planned to remove those. Lack of equivalent principle in overseas domain name systems is irrelevant.

11. Do you think the 'first come first served' principle should be modified and retained as an operational guideline?

Submitter	Summary of submission
Anonymous - prior work in domain names	**Supports modification and retention as operational guideline.** Provides quick low cost facility for registering domain names.
Blacknight	**Supports modification and retention as operational guideline.** Core principle for domains. Removing it would be dangerous.
Dreamscape Networks	**Supports modification and retention as operational guideline.** Agrees prior incarnation was not optimal
OFLC	**Supports modification and retention as operational guideline.** Suggested modification: **First come, first served:** A domain name will be registered on a 'first come, first served' basis if it is unregistered, available for registration and is in line with Internet NZ policies. Would mean that there needs to be a clear policy on domain names. Outside of te reo Māori considerations, there will be other words or phrases that should be unacceptable. The policy should be clear on what makes something unacceptable (e.g. a domain name that is clearly advertising what could be illegal material etc).
Edwin Hermann	**Supports retention as operational guideline.** Does not support introducing a list of banned words (words that cannot be registered as part of a domain name). Freedom of speech and freedom of expression is not only a human right but a value our society holds deeply. This is the case for pretty much all free and democratic countries. Banning words a direct attack of freedom of speech and freedom of expression and should not be tolerated. It is shallow-thinking at best, and a dangerous and slippery slope at worst. Will only contribute to the erosion of freedom of speech that many Western countries are seeing (e.g. cancel culture, political correctness, compelled speech bills). Does not solve any issues. NZ is a free country, a democratic country, a progressive country.

	Policies should reflect that.
Frank March	**Supports retention.** If we are looking for principles superior to mere operational guidelines, hard to go past first come first serve.
Ben Bradshaw	**Supports retention.** First come first served does not mean that there cannot be restricted domain names but that these restrictions are not pre-emptively applied. Any word filter system will cause unexpected restrictions. Funny example is always Pen Island. Human appeal process is necessary.
David Farrar	**Supports retention.** Would allow for certain names to be banned as domain names. Submitter chaired the Policy Committee in the early 2000s which rescinded the policy banning seven obscene words from being registered. Numerous reasons for doing so. Happy to elaborate in detail. One reason was that such bans are simple to get around. Instead of fuck.nz someone registers ck.nz and delegates fu.ck.nz. Likewise if you banned DPFisawanker.nz someone could register anker.nz and delegates DPFisaw.anker.nz
Arran Hunt	**Supports retention.** Can understand the thinking behind modifying this principle. But cannot support it - unclear how it would work in practice. Names could be reserved so they cannot be registered but unclear on what grounds they would be selected or who would decide who they could be eventually granted to. Can understand protecting the names of iwi and hapū, despite protections already existing in legislation and common law, would it extend further, to words or terms that are more encompassing to all Māori, and who would make the choice on who was allocated the domain and on what grounds? Would it extend to other groups of people? These are questions that there should be answers to before it is removed from being a principle.
Jannat Maqbool	**Supports retention as an operational guideline.**
Jay Daley	**Supports modification for clarity and retention - but as a guiding principle.** Does not support identifying words that would not be freely available for registration. All the registry sees is a domain name made up of letters, number and hyphens. It is rarely possible to correctly impute any meaning to that collection of characters until it is somehow used and that usage observed. What the first-come-first-served principle means is “wait until that usage is observed before making any decision on the legitimacy of that registration”. From that comes a set of implications that raise this into a guiding principle.

1st Domains	**Supports modification and retention as operational guideline.** Supports introduction of a reserved / prohibited name list if required.
MarkMonitor	**Supports first come first served principle for existing extensions.** For future launches would prefer if a system acknowledging registered trademarks and IP would be adopted to prevent unnecessary “clash” or unavailability.
DNCL	**Supports retention.** It serves well as the underlying principle and it would apply to domain name registration unless something else in the Policy specifies otherwise. It also works well in indicating that there is no hierarchy of rights (e.g. trademark owner does not have priority in registration of a domain name than a business owner). Removing this principle, without replacing it, would require a root and branch review and overhaul of DCNL and may be inconsistent with ICANN requirements and the stability, trust and security of the DNS and historical precedents determining registrants’ rights.

12. Do you agree that the ‘registrants’ rights come first’ principle should be removed?

Submitter	Summary of submission
Dreamscape Networks	**Supports removal**. Have the highlights noted within the more holistic set of principles.
Jannat Maqbool	**Supports removal [or retention as operational guideline]**. Principle is more operational.
Jay Daley	**Supports removal**. Operation of a ccTLD requires a complex balancing of rights between multiple stakeholder groups and a narrow statement like this is counter to that reality.
1st Domains	**Supports removal**. Covered throughout the operational guidelines.
Anonymous - prior work in domain names	**Does not support removal**. Domain names are effectively a form of property. Should only be lost following the decision on the basis of facts judged by a competent authority.
DNCL	**Supports retention and modification**. The description currently is only “the rights and interests of registrants are safeguarded”, which does not match the impression that the principle indicates.
David Farrar	**Supports retention and modification**. Registrants rights principle is important, while seeing the current wording is imperfect. The rationale behind it was to ensure policies did not allow registrars to trap registrants by refusing to transfer domains etc. Personally I always saw this principle as being more about guiding policies to be in the “public interest”. So happy for it to be formulated better.

13. Do you agree that the 'low barriers to entry' principle should be removed? Why / why not?

Submitter	Summary of submission
Dreamscape Networks	**Supports removal**. Actively support the promotion of a healthy and competitive landscape but concerned with the future state of security and reliability. Cannot be achieved with an environment that considers "low barriers to entry". Also a vastly different market than it used to be. Entrants without sufficient capabilities around technology, resources, budgets, etc. add little to the competitive environment but there are plenty of potential entrants with those capabilities in addition to security and stability.
Jay Daley	**Supports removal**. Despite claims to the contrary, .nz does not have low barriers to entry. .nz actually has high barriers to entry compared to the many TLDs where all it takes to become a registrar is a cheque in the post. There are probably other TLDs where the principals of a company applying to be a registrar must have been active in the industry for three years or more, but doubts there are many. High barriers to entry have kept .nz safe and secure far better than any other part of the .nz policy as they have ensured that we have a committed, knowledgeable and well engaged registrar population.
1st Domains	**Supports removal**. Could contradict moves to introduce industry minimum security standards / features / platform practices.
OFLC	**Supports removal**. Understands and supports the rationale for this, particularly as it pertains to the impact on a 'more secure, safe and trusted.nz'.
Jannat Maqbool	**Does not support removal**. No harm in reinforcing accessibility.
Anonymous - prior work in domain names	**Does not support removal**. Not until the plans for this are further expanded and it is shown how low barriers to entry are at odds with it.
MarkMonitor	**Does not support removal**. Should retain low barriers to enter the .nz namespace.
DNCL	**Does not support removal**. It is an important competition policy consideration. A very large variety

	of conditions and behaviour can affect the ease of entry into the domain name market.
Ben Bradshaw	Removing limits on pricing could allow for increased pricing for new development but it could also allow for straight old increased pricing. Does not know how diverse the true number of DNS registrars is and of this might be a competition issue.
David Farrar	Does not understand the assertion that having low barriers to entry may impede having a more secure, trusted and safe .nz. To respond more fully to this, needs evidence behind the assertion.
Arran Hunt	Reason for removal seems to be aspirational but not at all defined. Competition between registrars a good thing. Instead it is proposed that there is a “focus on openness in the .nz domain space more generally” and a focus on a “more secure trusted and safer .nz”. There is no indication as to how any of that is achieved by principle of maintaining a low barrier to entry.

14. Do you agree that the ‘no concern for use’ principle should be modified and retained as an operational guideline?

Submitter	Summary of submission
Anonymous - prior work in domain names	**Supports modification and retention as operational guideline**. Illegal activity should be removed from the .nz space.
CERT NZ	**Supports modification and retention as operational guideline**. Should be modified to enable cooperation with DNCL and trusted notifiers (i.e a set of rules to ensure copycat domains identified (eg: C3RT.NZ vs CERT.NZ)
Dreamscape Networks	**Supports modification and retention as operational guideline**. Arguable whether needs to be retained or encapsulated into other principals. Important call out particularly in an environment where further digital adoption is bottlenecked by the perception of complexity and difficulty.
Jannat Maqbool	**Supports modification and retention as operational guideline**, More operational.

Edwin Hermann	**Supports retention as operational guideline**. DNCL and InternetNZ should not be the judge and jury on the use of a domain name. InternetNZ should instead establish close working relationships with law enforcement agencies and related authorities, such as the SIS, GCSB, the Police, DIA, InterPol, etc. Problem with your proposed wording in the Options Report (page 31) is that it is far too vague to lead to any consistent interpretation.
1st Domains	**Supports modification and retention as operational guideline**. New wording would allow DNCL to be more responsive in responding to illegal activity, whilst not becoming overbearing in its power.
OFLC	**Supports modification and retention as operational guideline**. Principle would not sit well with the set of proposed guiding principles and could be seen to send the wrong message, particularly alongside the new proposed principle around safety.
MarkMonitor	**Supports modification and retention as operational guideline or complete removal**. Principle no longer reflects current attitudes of Registries in relation to "content" of domains. Should be modernised to reflect actual attitudes (as NZ has a proactive approach to content review) or removed completely.
Jay Daley	**Does not support modification and retention as an operational guideline**. Would go further and remove this principle entirely. Supports the proposed substitution of this with "The ccTLD manager should keep restrictions on the way domain names can be used to the minimum necessary to enable the .nz domain to be trusted and safe".
DNCL	**Supports retention as a guiding principle**. The DNCL does not support such move as it would alter the neutral role that the DNCL and InternetNZ has in facilitating the way the domain names are used.
Ben Bradshaw	Submitter made comments above around no concern for use. Would support a system which would allow trusted agencies OFLC, NZ Police, CERT NZ etc. to report domains and those could be blocked case by case. Not sure if it requires a policy change to implement. Would also support a public reporting mechanism of the number of domains blocked per month (by requestor) so we could have some accountability.

David Farrar	**Strongly against modification**. Would allow DNCL to decide if the use of a domain name is harmful, based upon assertion by certain agencies. If the status quo is not seen as acceptable, preferred changes in order are: 1. Law change to allow District Court Judges to issue a takedown or suspension notice of a domain name upon written application. 2. Law change to allow agencies mandated by Parliament to instruct DNCL/Internet to remove domain names. This means those agencies are the decision makers, not InternetNZ/DNCL, and they bear the liability and reputational risk of wrong decisions. 3. A policy allowing InternetNZ/DNCL to suspend a domain from the zone file for a short period of time (say max 72 hours) if they judge not doing so would cause overwhelming and irreversible harm. Would give an agency enough time to them follow the rule of law and apply for a longer or permanent suspension from a Judge Again the experience of a "concern for use" regime in .uk is we would expect such a regime here to have around 1,200 domains taken down every year and 89.9% of them would be related to intellectual property complaints.

15. Do you agree that the 'structural separation' principle should be retained as an operational guideline?

Submitter	Summary of submission
Anonymous - prior work in domain names	**Supports retention as operational guideline.**
Blacknight	**Supports retention as operational guideline**. The 3 R model (separation of Registry, registrars, registrants) is the one that is used internationally and avoids conflicts. A registry and its policy and administrative functions can focus on high level issues like those outlined in this review. Let registrars and other commercial entities deal with selling the domains and monetizing it.

Dreamscape Networks	**Supports retention as operational guideline**. Wholeheartedly agrees with the panel’s recommendations.
Jannat Maqbool	**Supports retention as operational guideline**.
David Farrar	**Supports retention as operational guideline**.
OFCL	**Supports retention as operational guideline**.
Keitha Booth	**Supports retention but as guiding principle**.
1st Domains	**Supports retention as operational guideline**. Important to maintain the structural separation between regulatory, registry and registrar functions. Healthy challenge and testing of these functions in the past. important to retain independence.
MarkMonitor	**Supports retention as operational guideline**. Need to retain clarity and scope of roles.
Liverton Security	**Supports retention as operational guideline.** InternetNZ should not operate as a registrar in competition to current registrars. InternetNZ has a role to require registrars to comply with minimum standards. If it is also operating as a registrar there is potential for InternetNZ to be compromised or conflicted.
DNCL	**Supports retention as operational guideline**. Many risks arise if the separation safeguards are removed. There are conflicts of interest when any company functions as both registry and registrar for a TLD. For example, it could subsidise its profits generated by its registry operations. It could lead to less competition, narrower choices, and poor consumer complaint handling practices because of less oversight functions.

16. Do you agree that the ‘clear chain of relationships’ principle should be retained as an operational guideline?

Submitter	Summary of submission

Blacknight	**Supports retention as operational guideline**. The 3 R model (separation of Registry, registrars, registrants) is the one that is used internationally and avoids conflicts. A registry and its policy and administrative functions can focus on high level issues like those outlined in this review. Let registrars and other commercial entities deal with selling the domains and monetizing it.
CERT NZ	**Supports retention as operational guideline**. Establishes contractual relationships for DNCL to establish responsibilities.
Dreamscape Networks	**Supports retention as operational guideline**. More transparent and easier to understand environment benefits all stakeholders.
Jannat Maqbool	**Supports retention as operational guideline**.
Jay Daley	**Supports retention but as a guiding principle**. Does not support retaining as an operational guideline if operational guidelines can be set aside in exceptional circumstances. If this principle (or first come first served principle) were set aside then that could easily mean a different market structure for .nz. Such a decision should only be taken with full public consultation and clear explanations of the implications of the new structure. Should instead create a new guiding principle about the fairness and transparency of the market structure, such as ".nz should operate with a market structure that is fair and transparent to all participants".
1st Domains	**Supports retention as operational guideline**.
MarkMonitor	**Supports retention as operational guideline**.
David Farrar	**Supports retention as operational guideline**.
OFCL	**Supports retention as operational guideline**. Makes sense to retain the clear chain of relationships and provide for a mechanism for the DNCL to intervene in the relationships where necessary.

17. Should the Panel consider any other principles?

Submitter	Summary of submission
CERT NZ	What is the most acceptable threshold test which would satisfy the DNC of the grounds for take down, short of a production order, warrant or similar? This should allow the DNC to agree, on balance, that the information supplied by CERT NZ is sufficient to take the domain down. This mechanism should allow for takedown in hours as opposed to days. It will also safeguard the DNC against unilateral or arbitrary actions, while at the same time improving cyber resilience.
Dreamscape Networks	The revised set of principles create a clear and well rounded divide of the stated goals. At an operational level there could be some consideration around ease of access, utilisation, application of process and policy to clearly place obligations on registrars (and the registry for arguments sake) to ensure that the space is as frictionless as possible. Whilst we are mostly good actors it is not complete. This would back off the “open and accessible” guiding principle and give substance behind it at that operational level.
Jay Daley	Proposes two new guiding principles: • .nz should aim to fairly balance the legal, moral and cultural rights of all stakeholders based on how the domain names are used • .nz should operate with a market structure that is fair and transparent to all participants.
DNCL	DNS stability – given the importance to the New Zealand economy it is important that the DNS of the Internet remain stable

18. Is there anything else the Panel should bear in mind when making recommendations on the principles or operational guidelines for the .nz policies?

Submitter	Summary of submission
CERT NZ	Any principle that improves the security of .NZ CERT NZ support.
Dreamscape Networks	Not beyond what has already been mentioned or considered. It is pleasing to see this level of engagement and collaboration to shape the future of the space.
Frank March	Two fundamental (de facto) principles are in operation now: 1. Regulation should be limited to the minimum requirement for effective functioning of the domain name system; 2. InternetNZ (or ISOCNZ as it was at the time) should be responsible for ensuring the addressing function worked effectively but not for what uses or services that function enabled. Another would be that, while InternetNZ itself might well be concerned about the greater good of humanity, or at least that portion of it dependent on safe and secure operation of the (NZ) Internet, the DNS operation is but a small (albeit critical) part of the whole. Management/managers of .nz should stick to their knitting. The review discussion paper more or less adheres to the above (in as far as they constitute 'principles'), except where it attempts to extend the role of the .nz manager well outside its sensible areas of real concern and responsibility.
Jay Daley	Without seeing the international review, it is hard to tell if that was sufficiently comprehensive and/or correct to properly inform the panel.
MarkMonitor	The lack of prioritization of trademarks and the lack of clarity on the conflicted domain names led to many missed opportunities and issues during launch. We shall explore this further in other questions.

DNCL	There should be a Policy Meta Policy that clearly defines policy terminology. Whatever changes are made should be made clear.
David Farrar	Keep it simple.
OFLC	Would be helpful for the Panel to consider ‘how’ the changes or recommendations should be implemented, including whether any stakeholders could be engaged further to strengthen the work. Anticipates that, should what is proposed go ahead, that this will mean significant change for InternetNZ/DNCL. Submitter would be happy to be engaged in discussions about any area of implementation that we may be able to assist with to assist with the change process.

Responses to the web video “New guiding principles for .nz”

These submitters responded to the video on the new guiding principles for .nz

Submitter	Comments
Jacinta	Current process allows blatant hate speech remain associated with .nz. I have made a complaint to you but menacing and vicious content remains online. The Christchurch Call is stronger. Please subscribe to the content and spirit of the Christchurch Call as a matter of policy and process. Feel free to email me for further details about my complaint and the inadequate response. People have been killed and the inspiration was thinking nsuch as that shared on a .nz domain. Are you really content to let that continue to be the case? Is there no-one in the employ of this company prepared to take action?

Nick	While the new principles may be potentially "better", you still need to be clear that some or all of the existing principles are implied by various of the new ones. The existing principles are all important, and it should not be possible for anyone to argue that the new principles in some way permit or necessitate abandoning any of the old ones. The new ones are broader and more abstract, and are therefore potentially more useful in guiding responses to new situations, however they must not be able to be used to significantly modify current practice in a way that would breach the current principles.
Stacey	I like the new ones, especially agree re: te reo & being more concerned about use. Possibly depends on the requirement needed to satisfy whether or or not a page is 'of benefit to New Zealanders'.
Jeremy	I think the new principals are really very vague compared to the old ones. For example, first come first serve. This is extremely clear. be open and accessible. This is not clear by itself at all and requires a lot more description to be clear. But worse than that, it is open to interpretation. ● be operated for the benefit of New Zealanders ● support te reo Māori and participation in .nz by Māori. I support these principles but again they require a lot of description. They could be more clear. ● help enable New Zealand to grow and develop. This is pretty meaningless. It's either inherent or it or requires a plan behind it.

The .nz domain space and Māori

48. Should there be a requirement to take reasonable steps to engage with Māori when amending the .nz policies?

49. Should InternetNZ ensure it has adequate capability to facilitate engagement with Māori?

50. Are there any other .nz-related issues affecting Māori that you think should be considered?

Submitter	Should there be a requirement to take reasonable steps to engage with Māori when amending the .nz policies?	Should InternetNZ ensure it has adequate capability to facilitate engagement with Māori?	Are there any other .nz-related issues affecting Māori that you think should be considered?
Anna Pendergrast	**Yes**. Both as a direct result of this review and in future amendments. Māori engagement should be a priority. Further work on developing new re-writing of policies should be paused until there is appropriate Māori engagement in place – this cannot be an add on to the process.	**Absolutely**. This should go beyond having one person on staff as a Māori engagement lead or similar. Capability needs to be built throughout the organisation and additional capacity requirements identified and prioritised.	
Anonymous -	**Yes**. In administering the .NZ	**Yes**. In administering the .NZ	**Unknown**. As a surrogate for New

prior work in domain names	name space on behalf of all of New Zealand, InternetNZ should act in accordance with the Treaty partnership.	name space on behalf of all of New Zealand, InternetNZ should act in accordance with the Treaty partnership.	Zealand society, our Treaty obligations need to be met by the administration of .nz. Does not have sufficient knowledge in this area to have useful input. Panel has already considered a number of issues the submitter did not know existed before reading the Options Paper.
Ben Bradshaw	**Yes**.	**Yes**.	Not qualified to talk to this point, but has not ignored it.
Blacknight	**Yes**.	**Yes**.	
DNCL	As mentioned above, the DNCL wishes to wait for the Panel's and the community's further feedback.	The DNCL notes from the Panel's issues paper that the panel found strong support to protect te reo in the .nz space from its stakeholder engagement but mixed feedback on whether there should be a strong connection to Te Tiriti o Waitangi (the Treaty of Waitangi) and .nz.	
Dreamscape Networks	**Yes, absolutely**. Arguable that InternetNZ would be doing itself and its mission a disservice by not doing so.	**Yes**. Otherwise it serves as a potential distraction from the other goals and objectives of InternetNZ and/or diminishes the level of focus across each of the items, Māori engagement included.	**No**, not which submitter could currently highlight.

Edwin Hermann	Important to engage with Māori. But should not be done at the expense of engaging with the wider New Zealand public. All views matter. InternetNZ should develop an engagement strategy with Māori but also include wider engagement to ensure that feedback from all sectors of society is sought.		
Jannat Maqbool	**Yes but** with other cultures also.	**Yes but** with other cultures also.	No
Jay Daley	**Yes**. See response to q11 for more details. Opportunities to enhance .nz growth and improve market operation.		
OFLC	**Yes.** Engagement with Māori is a critical step in honoring the principles of Te Tiriti o Waitangi and will strengthen any proposals to take forward for the betterment of all NZers.	**Yes** – this is an important area – Māori are the indigenous people of New Zealand, and therefore should be respected as such. The digital nature of our lives now impacts and affects Māori in different ways than it may do for pakeha and understanding this is important to be able to truly realise an inclusive future for .nz.	There likely will be and it would be our view that consultation with Iwi will help to identify these areas.

Access and openness

Issue one: The .nz policies are written only in English

- Option A: the current situation
- Option B: Make the policies available in te reo Māori as well as English
- Option C: Make the policies available in te reo Māori and take other accessibility measures like adding other languages over time according to how widely used they are

Submitter		Summary of Submission
Blacknight	B	Supports option B. The option could however cause issues if there are differences of interpretation between the two versions of the texts. Some countries state that one language is definitive when there is a conflict.
MarkMonitor	B	No reasons given.
1st Domains	B	Supports option B. It is the right thing to do and follows the openness and commitment to Māori principles. Does not agree however that the current .nz policies are highly technical and having them written in English only could be an impediment to registration of a .nz domain name. Registrar website and service offering are likely to have more influence on registering a .nz domain name than how policies are written and in which language.
Jay Daley	B	Supports an amended option B. Policies and content should be provided in or fully support the three official languages of Aoteraoa. That means all words translated into English and te reo Māori and all video/audio content close-captioned.
Keitha Booth	C	Supports active use of Te Reo in the .nz domain and a partnership with Māori to achieve this. Then move to represent NZ's full ethnic mix.
Jannat Maqbool	C	Supports option C. Need to value all languages of the people of NZ.

CERT NZ	C	Submitter is creating multiple Pacific language translation of its key resources and would be pleased to see its partners do the same.
Anna Pendergrast	C	Supports option C. The policies should be made available to as many people as possible and reflect the official languages of New Zealand and a commitment to accessibility that is a core part of digital inclusion. Generally comfortable with all options but considers “high usage” should not be the only measure for additional languages. Also thinks we should consider NZ Sign Language early on as an additional language and the format in which the principles are published. For example, instead of putting everything in PDF documents which are hard to navigate, we could have easily navigable HTML content (see govt.nz webpage for example).
Edwin Hermann	C	Does not consider options B or C will achieve greater access for people who do not speak English. A third option would be better. Make the policies available in English and add other languages over time according to how many people do not already speak any of the languages in which the policies are currently available. Option B would not achieve greater access because all (adult) speakers of Māaori also speak English. Data from the Census should instead be used to determine which language is next most commonly spoken of the NZ population that does not speak English. Process could be repeated to gradually increase access to a greater and greater proportion of the New Zealand population.
Anonymous - prior work in domain names	C	Not opposed to option C in principle. Notes difficulty in determining whether other languages are widely used in New Zealand.
DNCL		The DNCL agrees with the assessment of the options. We suggest that the language options should reflect the current languages accepted by the NZ passport office and the New Zealand Transport Office for drivers’ licenses.
David Farrar	C	Supports option C but need to be clear about which version is the primary version, and which is a translation. Translations are rarely exact and we need clarity.
OFLC	C	Supports option C – having policies in Te Reo and English – with the commitment to add other languages overtime is a really positive step and supports making .nz accessible. Acknowledges adding other languages over time would have a higher implementation cost than other options.

		Something that could slowly be added to over time to reduce initial overhead, whilst still showing progress.

Issue two: Lack of availability of characters other than English and te reo Māori alphabets in .nz domain names

- Option A: the current situation
- Option B: support additional characters as demand arises
- Option C: support all characters for most widely used New Zealand languages

Submitter		Summary of Submission
Berend de Boer	A	Supports option A. NZ has two languages. .nz domain so Nzers are the target. People that come to New Zealand are expected to speak English (requirement for permanent visa).
CERT NZ	A	Supports option A. Preferable from a security perspective as it prevents homoglyph attacks.
Jay Daley	A	Supports option A. Many ccTLDs allow multiple character sets without registry or registrar staff generally being able to read the languages those characters are used for. This is introducing significant problems leading to a narrowing of the policy. Disagrees that Option A would mean “No improvement in trust in .nz.”. Taking a different option could reduce trust in .nz.
Anonymous - prior work in domain names	A/C	Supports A and C. Not sure how demand for B would be assessed.
Ben Bradshaw	A/B	Supports option A or B. Option C adds a new range of security concerns and could impact trust in the .nz space if people are seen to be registering lookalike domain names to run phishing attacks.
Blacknight	B	Supports option B. Adding support for other IDN tables only makes sense if there is demand to do so. Option A would be limiting and would ignore demand. Option C would lead to unnecessary

		cost with little benefit. Option C was considered during the addition of IDNs in the .ie namespace but decided to keep the focus initially on our national language only. The uptake has been very low. Had more languages been added the investment would have been wasted.
Michael Homer	C/B	Supports an alternative option. Would prefer the maximal widening of codepoints even beyond options A-C, and only option B as proposed permits that expansion. However, a somewhat-extended option C-then-B would be ideal. Supports permitting a range of diacritics used with Latin characters within English text, in loanwords (café, föhn, jalapeño), and in proper nouns, characters as a group in the early phase as well if security concerns can be addressed. These represent a relatively-small number of characters but enhanced accessibility for some uses, while also covering a range of Latin-script languages in one go. Expects that any demand-based process would result in most of these being included eventually anyway. Symbol-based domain names are of questionable usability but should be considered, even if ultimately dismissed.
1st Domains	B	Supports option B. We should observe other ccTLDs (like .com.au) as they introduce IDNs in their Registry before introducing new characters to .nz. Will allow us to estimate demand and adopt a proven and tested approach to dealing with any security issues. 1st Domains does not currently support IDNs and has received very limited requests over the years to register them. Therefore, we should adopt a ‘wait and see’ approach before advancing IDNs further in .nz beyond what is already supported.
Jannat Maqbool	C	
MarkMonitor	C	
Anna Pendergrast	C	Supports option C. On the assumption that security risks can be appropriately mitigated.
Edwin Hermann	C	Supports option C of the options put forward. Provides the most flexibility and best reflects the multicultural nature of New Zealand. Additionally, the advantages outlined in the Options Report for this option also far outweigh the disadvantages.

		Prefers a fourth option that has not been considered: support any character that is encodable using Punycode. All other options limit the choices available in some way. It is not clear why, nor what advantage this provides over supporting all characters.Allowing any character (provided it is encodable using Punycode) would provide the most choice, provide the most freedom, and meet the needs of as much of the population as possible.
DNCL	C	
OFLC	C	Supports option C. Most inclusive option. However, understands that this would be more complex and costly to implement and can attract greater security risk. For those reasons, would support option B with a view to moving to option C if demand was high enough over time. In option B, would still need to work through security implications and should do so with an eye on protection for a future for option C.
David Farrar		Market research should be done to determine potential demand for an expansion, before decisions are made. Is this a solution looking for a problem or are there significant numbers wanting further IDNs. Tends to support more characters being available, so long as non-malicious use will be significantly greater than malicious use.

Issue three: No geographical limits on registrants

- Option A: The current situation
- Option B: Educate .nz users that .nz domain names can be held from anywhere around the world
- Option C: Impose a local presence requirement

Submitter		Summary of Submission
MEGA	A	Supports option A. Current situation is working satisfactorily. No significant changes are needed. Significant number of overseas entities operate .nz domains, often replicas of their primary domain, so it is too late to think that “there is a risk that .nz users will receive a surprise about who can hold a .nz domain name, leading to reduced trust in .nz....”

		Option B would not result in any meaningful improvement on the current situation. Instituting and ensuring compliance with option C would be extremely costly and time consuming. DNCL resources could be better focused in any number of other areas. Option C would also raise the issue of how to deal with current registrants who may not be able to meet the new eligibility requirements to hold a .nz domain. If they were allowed to continue to hold their .nz domain registrations in the interests of fairness and commercial certainty, some of the supposed benefits of instituting the eligibility requirement would be undermined. Also unclear how to treat a New Zealand owned entity with a .nz domain that became wholly or substantially owned by an overseas party. Or how to determine what degree of overseas ownership or control would be regarded as being incompatible with satisfying the local presence requirement. If a registrant wholly or partially acquired by an overseas party was allowed to continue to hold their .nz domain, which practically speaking in the interests of fairness and commercial certainty they would have to be, some of the intended benefits of instituting a local presence requirement would be undermined. If the conditions for register under option C were too onerous, it may deter legitimate overseas businesses wanting to target New Zealanders from looking to register and trade through a .nz domain. This would be commercially detrimental to the .nz domain market, including by reducing the competition for and trade in .nz domains and consequently also innovation in the space. If the conditions were not onerous enough, it may not significantly reduce the number of bad faith actors holding .nz domains, undermining one of the key intended benefits of instituting the requirement. Even if a workable and effective local presence requirement was introduced, in many cases it would still be difficult to hold an overseas-based person to account for .nz-related conduct, undermining one of the key intended benefits of instituting the requirement.
1st Domains	A	Supports option A with an opt-in local verification option. Should retain the current situation but offer an extra level of local verification or certification to participating individuals / organisations. This could be in the form of a centrally operated (InternetNZ) .nz trust seal that could be displayed on websites, linking back to an authoritative website that can provide verification. Additional information could be collected via the Registrar such as NZBN, verified contact details,

		RealMe identity verification, drivers' licenses etc and processed via API. A centrally operated website would allow internet users to enter a website address and verify its status, and the website operation to display a dynamic .nz trust seal on their website providing an additional level of trust for .nz. Does not support imposing a local presence requirement. Would add complexity, cost and increase entry barriers to .nz. Registrants have choice. With unrestricted gTLDs now numbering in their hundreds, adding additional hurdles to gain a .nz domain name would reduce their appeal. Retrospectively imposing a local presence would be challenging to implement given the long time we have been operating an open ccTLD. People determined to deceive and act fraudulently will find ways to bypass any checks. Any additional measures may just add extra governance without adding any real value or protections. If DNCL has adequate monitoring and powers to regulate unacceptable use, .nz can still maintain its reputation as a safe ccTLD whilst staying open.
MarkMonitor	A	
Anna Pendergrast	A	Supports option A. Unclear what the level of current .nz domain use is from people and organisations without a New Zealand link and therefore what risk can be expected from having a "NZ link clause". Having these types of restrictions is complicated, time consuming to implement and potentially exclusionary if not scoped appropriately. Not necessary to do wide, proactive communications to inform domain name holders that "anyone can have a .nz domain".
DNCL	A	Submitter holds dear the liberalisation of rules with registration, making the process accessible across the world.
David Farrar		Advises against option C. Would go against a clear trend globally of fewer restrictions. Would also mean either the cancellation of thousands of domains or grandfathering of them, undermining any benefits. Would also add cost and complexity registrations.
Arran Hunt		Against option C. The cost in implementing and maintaining the system would discourage its use. As NZ internet users will not limit their internet use to merely .nz domains, it will not necessarily provide any more safety to them. If implemented it would just lead to people in NZ registering domains on behalf of people overseas.

Herman Edwinn	A/B	Supports option A or B. Solution to the problem of many people thinking .nz domain names are only registrable by NZ entities would best be addressed by education rather than policy changes.
Ben Bradshaw	B	Supports option B. Important for NZers to know that anyone can register a .nz and use it. It has never been a guarantee of a NZ presence and will never be. Option C is technically and humanly unworkable. Anyone with a goal to operate in NZ will be able to find someone in NZ to register the domain and then operate it.
Blacknight	B	Supports option B. One of the attractions of NZ is that it is open and inclusive. Educating New Zealanders about how it is open can only be beneficial. Option C is a terrible idea. The only way it could work would be to introduce a specific third level namespace with restrictions, as the horse has long bolted. Also most ccTLDs either have removed or are removing geo restrictions. NZ should not be going backwards.
Berend de Boer	C	Supports option C. Significantly increases trust in NZ domain.
CERT NZ	C	Supports option C. Current situation needs stronger controls as we regularly see .NZ domains registered overseas hosting phishing and malware.
Jay Daley	C	Supports option C. Serious consideration should be given to option C. Works well for Australia and many other countries and helps to maintain a safe and trusted namespace.
Anonymous - prior work in domain names	C	Supports option C. Supports a .nz presence requirement to give consumers added confidence when dealing with websites that have .nz in the name.
Michael Homer	C	Somewhat supports a modified version of option C. There are large numbers of overseas-based “squatters” occupying much of the .nz domain space. This change would eliminate that. However, incorporating a New Zealand company to act as legal owner is trivial and commercial operations likely would do so, so the true impact may be limited. The second potential variation for a local presence requirement described in option C is too strict

		for individuals but too relaxed for other entities. Individual New Zealand residents who are neither citizens nor permanent residents ought to be able to register domain names. The first branch, requiring “a legal presence in New Zealand” appears to permit this. Requiring that overseas entities only “trade in New Zealand” is too weak in the absence of further definition. Suggests 2 limitations: (1) individuals must be resident in New Zealand, New Zealand citizens or permanent residents; (2) entity registrants must be established, registered, or incorporated under New Zealand law. Option B is not a genuine option. There is no practical approach to this education in any meaningful way. It represents only a resource sink. Option A is adequate as the status quo.
Jannat Maqbool	C	Supports option C. It aligns with some of the other principles related to supporting NZ and NZers.
Commerce Commission	C	Supports option C. Many of the complaints the submitter receives about .nz domains relate to overseas entities. Has received 17 complaints since November 2019. about .nz domains registered to overseas addresses. Agrees that many NZers are unaware that overseas based registrants can hold a .nz domain. Consistent with the common narrative of complaints submitter receives where a consumer purchases from an overseas business thinking they were purchasing from a NZ business due to the .nz domain name. Agrees that it is difficult to hold overseas-based registrants to account for illegal conduct. Good example is Viagogo. Only accepted the jurisdiction of the NZ Courts following a Court of Appeal judgement. Very difficult for consumers affected by false or misleading behaviour to seek a remedy. Local presence requirement would also bring NZ policies into line with the Australian .au Domain Administration (auDA), which has an Australian presence requirement. Local presence requirement would significantly reduce (1) overseas based businesses failing to supply or supplying materially different goods to consumers (2) entities purchasing lapsed .nz domains, using a generic storefront and selling counterfeit goods from overseas (3) consumers mistakenly purchasing from overseas businesses thinking they were NZ businesses due to the .nz domain.
OFLC	C	Supports option C. Would protect from harm and ensure that those misusing the .nz domains can be held accountable. Supports option within C where the applicant is required to have some legitimate presence or connection in NZ.

		Could also be an option 2A. Supports educating New Zealanders on who can hold a .nz – and see public education as an important component of how we collectively reduce harm and provide good public information. Any education campaign about who can hold a .nz could/should be framed within a broader set of messages about the .nz environment. Submitter sees value in a public education campaign, regardless of what option is chosen.

Responses to the web video ".nz from afar"

These submitters responded to the video on whether there should be geographical limits on registrants.

Submitter		Summary of Submission
Robert	A	Supports option A. Option A may be making .nz less trusted, less secure and more vulnerable to dodgy stuff. But questions whether this is a hypothetical problem, rather than an actual, significant problem. Also questions whether we should be making policy changes around perceptions of potential problems.
Jacinta	C	Supports option C. Current process allows blatant hate speech to remain associated with .nz. Supports subscribing to the content and spirit of the Christchurch Call as a matter of policy and process. Made a complaint to the Domain Name Commission. Inadequate response to it. People have been killed and the inspiration was thinking like that shared on a .nz domain. Questions whether InternetNZ is really content to let that continue to be the case / take no action.
Jeff	C	
Bob	C	
Johanna	C	Supports option C. New Zealand brand must be protected in a world where the lines between real and "fake" are becoming increasing blurred. Need to keep .nz for those with a New Zealand connection to minimise the risk of harm caused by ruthless operators.
Brock	C	Supports option C. A New Zealand connection would stop anyone from randomly registering .nz domain names. This is the case with Australia's .com.au domain name. Good system as it stops

		kiwis snapping up Aussie domains. The same should apply on the .nz. ould give .nz a point of difference.
Rachel	C	
Justin	C	Supports a modified option C. Does not see much of a downside to keeping .nz a bit 'pure'. E.g only kiwi registered companies or n.z. citizens allowed. Supports a simple company, charity, or passport number requirement, with an exception route for others to justify their entitlement. Should be a stringent requirement for 'short' .NZ 2LDs. However, would be relaxed about leaving .co.nz 3LDs open as it is now.
Bernie	C	
Tony	C	
Richard	C	Supports option C. .nz should be just for kiwis and businesses in New Zealand.
Fiona	C	Supports option C. NZ is a trusted name and brand. We should keep it that way.
Stephen	C	
Liza	C	Supports option C. Can truly help when you see where an email comes from.
Dean	C	Supports option C. An anything goes ethos has come with globalization and unrestrained economic growth. Supports tightening everything up to make things ethical and get honest.
Paula	C	Supports option C to make it NZ only. Foreigners should not be able to get domain a .nz domain name because New Zealanders cannot get domain names from other countries. Would be too easy for criminals to use .nz and people would trust it because it is NZ. And then trust will decrease when people get scammed. So it needs to stay NZ domiciled users only.
Richard	C	Supports option C. It should be limited to a NZ citizen, nz registered company, society or trust.
Oliver	C	Supports option C. Despite education campaigns, most people will expect a NZ domain to belong to an nz entity. This is also a requirement for other tlds, like .de. Does not see the downside of requiring a nz connection but on the other hand potential for abuse/misleading behaviour.
Miles	C	Supports option C. Would like to see support for okina characters for Samoan and would also like to see support for Chinese symbols - for folks with an NZ connection. We may as well just allow

		any character from any DNS allowed unicode point.
Andrew	C	

Security and trust

Issue four: Domain and website content abuse

- Option A: The current situation
- Option B: ‘No concern for use’
- Option C: Suspension of a domain name on advice by a trusted notifier
- Option D: Implement an ‘acceptable use’ policy

Submitter		Summary of Submission
MEGA	A	Supports option A. Provides an appropriate balance between regulation and oversight being left to the courts and other specialised agencies such as the Office of Film & Literature Classification and the Digital Safety Unit of the Department of Internal Affairs, while still allowing for the continued operation of the ‘emergency circumstances’ powers. Option B does not allow for the continued operation of the ‘emergency circumstances’ powers, provides far too much of a ‘hands off’ approach to regulation in emergency or exceptional circumstances, where intervention is wholly justified and essential. Options C and D would require DNCL to police domain name use and content in a substantial way. Would entail extensive investment and focus, even with the assistance of ‘trusted notifiers’, which would distract from DNCL’s existing core activities, which should always be it’s primary focus. Ever-increasing importance of a domain name to a business as more commerce moves online, including where businesses like the submitter’s operate solely online via a domain name, the incorrect actions of DNCL in suspending a domain name, even if well intentioned, would have catastrophic effects for a business. Ever-increasing range of material and services represented online means it will also not always be

		easy to determine if illegal activity is being conducted through a particular domain name. The determination is much better left to existing, experienced and specialised entities like the courts and the government agencies mentioned above. Tasking DNCL with taking action against domain names being used legally but allegedly 'inappropriately', could have a chilling effect on freedom of expression. It is also impossible to decide what is 'inappropriate' particularly as such values in society continually change. Submitter has been incorrectly blacklisted, even by experienced agencies such as Microsoft, and the time it takes to reverse these invalid decisions can have significant commercial impact.
Edwin Hermann	B	Supports option B. InternetNZ should not be the arbiter on what constitutes illegal use. Banks do not freeze accounts because they suspect there is illegal activity taking place; NZ Post does not confiscate parcels simply because it suspects there is an illegal substance being imported into the country. These matters are instead referred to law enforcement agencies. Domain name registrations should operate in a similar way. InternetNZ should establish close working relationships with law enforcement agencies such as the Police, DIA, SIS, GCSB, InterPol, MPI, etc. Option C is also also a good option if the "trusted notifier" is a government agency and not some third-party organisation or private company. There is too much risk of manipulation or corruption if "trusted notifier" included private organisations.
Anonymous - prior work in domain names	B	Supports option B. Option A provides very little additional protection over option B. Option A had little to no effect on the ability of the Australian terrorist's supporters to promote their hate speech & distribute the video and manifesto. Option D is resource intensive and would require DNC to judge website content. Gives example of YouTube overreaching with their acceptable use policy. Option C also has problems. The Office of Film and Literature Classification already has the power to instruct removal of harmful content. Could allow that office to instruct that domains insisting on displaying harmful or illegal content be removed but not government departments parliament has not chosen to give equivalent powers to. They would need to demonstrate a need to a competent NZ court of tribunal. Concerned with the list of trusted notifiers. Trusted notifiers must be trustworthy and stay within

		their domains of knowledge. Example of 2013 parody on The Daily Blog of the police's inaction over the Roast Buster scandal. A police officer threatened the blog editor with fines and imprisonment if the parody was not removed. If police had been a trusted notifier they could have had the domain taken down. Criteria for being trusted would need to be considerably tightened if we pursued this approach. Human Rights Commission should be added to trusted notifier list as the obvious candidate in the field of human rights.
DNCL	B	Prefers option B, which allows the retention of 'no concern for use'.
Jay Daley	C	Supports option C. There are some high-quality organisations like Netsafe that are capable of being trusted notifiers.
Jannat Maqbool	C	Supports option C.
Hein Frauendorf	C	Supports option C. Need to be able to have nz domains used for phishing or other malicious activities suspended to protect the NZ Public.
1st Domains	C/ D	Supports a combination of options C and D. Will likely become necessary to outline some parameters of what acceptable use is in order to act on advice from these trusted organisations. There may be a grey area when it comes to compromised websites, where malware or phishing content has been placed on a legitimate website. There therefore needs to be a robust mechanism for advising, suspending and reactivating domain names where a Registrant has become a victim of cybercrime. The DNCL is taking a more proactive stance on domain and website usage but can only take down sites where registration data is also not valid. Policy should be extended so that they can act based on inappropriate usage but within well defined parameters. Another option to address malware and phishing sites could be that InternetNZ takes a more proactive role in maintaining clean websites in the .nz space. InternetNZ could partner with organisations like Google, to use their Google Safe Browsing data across all of .nz. An automatic notification mechanism via the Registrar could be used to notify a .nz Registrant when unsafe websites have been detected, similar to the DNS zone scans the Registry already performs.

		InternetNZ should look at ways to leverage its data and partner with other organisations that hold complementary data on .nz to innovate in this space.
Blacknight	C/D	Supports a combination of C and D. How domains are used cannot be ignored as this goes against the concept of it being a trusted and secure online space. Laissez faire policy might seem attractive but in reality it does not work. However, need to be clear lines around what kind of issues the registry will act on and which ones are out of scope. Issues of security and stability or other issues like child abuse, imminent physical harm etc. could be in scope but it the registry should not act as the content or trademark police.
CERT NZ	C/D	Supports option C as it will work towards making .NZ safe and secure. Option D would also be acceptable. Right to due process could be addressed through a “challenge to” process and policy.
Commerce Commission	C	Supports option C. Would provide far better protection for NZers and improve the overall security of the .nz domain system. Current system is too slow to address issues around domain and website content abuse. Online based harms can have an immediate effect and often require an immediate response. Waiting for direction from the Courts can seriously limit the ability to act swiftly, allowing ongoing harm and often the cost is prohibitive. Allowing the suspension of .nz domains used to facilitate illegal activity will act as a significant deterrent for these types of registrants and an effective way of preventing further harm. Would be helpful for DNCL to follow a similar approach to that of the auDA. (AuDA may suspend or cancel a license when it is in the public interest if two criteria are met: (1) request is received from an enforcement body or intelligence agency and (2) AuDA believes on reasonable grounds that the action is in the public interest. AuDA’s policy lists a variety of factors as public interest objectives – including consumer protection and the integrity, stability, or security of the Domain Name System.) DNCL adopting a similarly comprehensive policy would likely provide a transparent system where registrants would know what to expect and be treated fairly. Current system or continued adherence to the ‘no concern for use’ policy would contradict the Panel’s goal for a secure, trusted and safe .nz domain name space.
Ben Bradshaw	C	Supports option C. Supports a trusted notifier relationship while keeping InternetNZ and DNCL out of the decision making process for domain restrictions, allowing them to stay impartial. As noted above, a reporting framework to see how many domains each trusted notifier has restricted would

		help build trust and allow potential abuse of the system to be identified and queried by the public.
Arran Hunt	C	Supports option C if the advice is solely taken from the listed government departments and only implemented for the more serious of circumstances. Should ideally be in legislation and not left to InternetNZ. Government's decision to not put this into legislation should also be considered. Against option D. With the exception of illegal material, an "acceptable use" policy provides uncertainty unless very clearly drafted. Even then, it allows some people to push their views on others. Would be counter to the NZ Bill of Rights.
Michael Homer	D	Supports option D given policy goals. Option A also adequate under resource constraints. Every option is better than option C. Option C would delegate enormous authority to miscellaneous organisations without a clear process for determining these or having any insight into their internal processes.
OFLC	D	Supports option D. An acceptable use policy feels appropriate and sends the right message to those wanting to use .nz in our view. Appreciates the potential concerns in relation to Option D so would support Option C – but expect that there is also some guidance provided on what is not acceptable. Option C could be strengthened and pick up components of option D. Proposes adding the establishment of an 'acceptable use guideline' advertised and provided to all registrants that provides principles and guidance about things that the DNCL may consider taking action on in relation to misuse or illegal activity through a .nz domain. Potentially less 'limiting to freedom of expression' than what is proposed in Option D but sets some expectations upfront – and includes notification that the DNCL will act on advice from trusted notifiers.
David Farrar		InternetNZ/DNCl should not be judging acceptable use. Should either be left to judges or Parliament to legislate to give certain agencies the power to instruct a deletion or suspension. InternetNZ should not be taking on liability and risk and reputational issues on behalf of agencies.

Issue five: The interim emergency circumstances clause

- Option A: Allow the interim policy to lapse
- Option B: Make the interim policy permanent as it is currently phrased
- Option C: Modify the interim policy and make it permanent

Submitter		Summary of Submission
Edwin Hermann	A	Supports option A. Intentions good but introducing the interim policy seemed a knee-jerk reaction in hindsight. InternetNZ should not be the judge and jury over what constitutes illegal use. Should be left up to the law enforcement agencies that already do this. Correct way to tackle this problem is to establish good communications with these agencies rather than assigning InternetNZ powers that leave its execution open to abuse. Should apply the same principle as banks and NZ post, which do not freeze bank accounts or confiscate parcels unless a government agency or a court order instructs them to do so. Establishing close working relationships with good lines of communication is key to address expediency issues.
Anonymous - prior work in domain names	A	Supports option A. Concerned that there may be scope creep. In a genuine emergency it could be reinstated.
Blacknight	A	Supports option A. If option A is coupled with the adoption of an acceptable use policy it gives you a variation on option B. Probably a sane approach.
MarkMonitor	A	Supports option A. Would however like the registry to adopt a DNS Abuse Policy for domain suspension.
Ben Bradshaw	(A)	Would prefer a trusted notifier framework to be available in the future so would not seek to make this a permanent policy. Not sure how long it would take to set up a reporting framework but until that time 6 monthly renewals by the council would not be so bad if seen as needed.

MEGA	B	Supports Option B. As it is currently phrased, operation of the 'emergency circumstances' powers is essential and wholly justified in emergency or exceptional circumstances where use of a .nz domain is causing or may cause irreparable harm. Interim policy as it is currently phrased is adequate.
Jay Daley	B	Supports option B. Submitter refers to previous answer (q. 4) on harm. See Jay Daley's comments on page 16 of this paper.
Commerce Commission	B/ C	Supports continuation of the interim policy. No view on whether the policy should be modified. Measure vital in allowing prompt action during emergency circumstances. Particularly where the alternative relies on the judicial process. During Level 4 Covid-19. lockdown the Courts could continue as an essential service but decided that only proceedings affecting the liberty of the individual or their personal safety and wellbeing, or proceedings that are time critical, would be heard at this time. Likely that issues relating to Covid-19 and .nz domains would not be considered a high priority during such circumstances.
OFLC	B/ C	Supports options B and C. Current clause could be strengthened but useful as it stands. Important in either option B or C that there are some transparency and accountability measures in place. Would not support option A at all – some form of ability to intervene is important.
Jannat Maqbool	C	Supports option C.
Hein Frauendorf	C	Supports option C. Will help better protect the NZ public.
1st Domains	C	Supports option C. DNCL should have these powers to act under exceptional circumstances as regulator of the .nz space.
CERT NZ	C	Supports option C. Will ensure wording is appropriate through further discussion and feedback.
DNCL	C	Supports option C. The recent disasters have shown that the DNCL should be prepared for the worst. With plans to modify the policies, there would be more time to consider the details and to translate the interim version to be more general.
David Farrar	(C)	A power should exist but only for a short period of time such as 72 hours to give agencies time to go

		through a judicial process.

Issue six: Domain name registration abuse

- Option A: Current situation
- Option B: Introduce data validation for all domain name registrations
- Option C: Introduce data verification for high risk domain name registrations

Submitter		Summary of Submission
Anonymous - prior work in domain names	A	Supports option A. Other options would add additional costs and probably be futile. Unless registrars went to the trouble of verifying a physical address, it would be easy enough to fraudulently use someone else's name and address in contact details with an anonymous email address and throw-away phone number.
Blacknight	A	Supports option A. Causes the least friction. Expanding how the registry monitors the zone might help identify risks but it should not be the norm to add a burden or obstacle to registration. Option B a bad idea and would cause more problems than it resolved. Now clear what "high risk" is under Option C. Several ccTLDs have tried to use variations on this and it causes more problems than it solves while also giving a false sense of security. Exception would be domains identified as being algorithmically generated for use in botnets etc., however this would probably be covered in other parts of the policies.
Jay Daley	A	Supports option A. Data validation would only work if: • There was a single, consistent addressing scheme for New Zealand if local requirements are introduced and also for the rest of the world if not. • There was a national identity scheme if local requirements are introduced and a global one if not. • Criminals promised not to use fake data. • There was a definition of a "high-risk" domain.
1st Domains	A	Supports option A. Attempting to verify or validate contact information will increase costs and be difficult to implement across all Registrars. Even verifying that a physical address exists can be

		difficult. There can be many inconsistencies with address data provided by various organisations, especially businesses. Supports attempts to make data received more consistent in its format, and therefore, more easily verifiable by DNCL. InternetNZ could provide APIs/Tools to be used to verify collected data at time of entry to provide real time response to the customer. Another option like option C would be to review high-risk domain names after they have been registered, rather than pre-determining them. Otherwise, in option C there is an assumption without evidence that there is potential for abuse and preventing registrations.
MEGA	A	Supports option A. Current system is in line with the majority of top-level registration systems overseas, so the risk of abuse is no greater than other top-level domain names. Introducing requirements of validation and/or verification of registration information would be a time consuming and costly process, which would still potentially be open to abuse from motivated parties. It would also delay new registrations across the board, including by legitimate registrants, which could inhibit the growth of .nz.
DNCL	B	Supports option B, particularly the statement that the validation should occur at the time of registration. Ideally, verification will be performed as well, but that would create a significant burden on the DNC to verify each application. Agrees with Panel’s assessment of situation, but notes there are other models available that can potentially reduce data registration. The DNCL believes that data validation at the time of registration is the best approach.
Jannat Maqbool	B	
Hein Frauendorf	B	Supports option B. We need validation and verification. Domains considered low risk can and will still be used as attack vectors against the NZ public.
CERT NZ	B	Supports option B. Option C could work if high-risk domains could be adequately identified and

		separated. Option A is not sustainable given the level of abuse happening in NZ environment.
Edwin Hermann	B	Supports option B, unless the cost is prohibitive. Well-thought-out option because it helps make .nz more trust and secure, and yet in doing so does not impinge on anyone’s freedoms or rights.
Office of the Privacy Commissioner	B	Supports Option B Applicant data should be validated before the application is granted. Consistent with Information Privacy Principle 8, which requires that reasonable steps are taken to ensure that personal information is accurate, up to date, complete, relevant, and not misleading. Should verify data like applicant contact details to reduce the risk the applicant cannot be contacted in an incident. E.g., requiring verification emails to be sent. Data such as the proposed domain name should be validated against a restricted character set. This would reduce the risk of homographic compromises and is consistent with Information Privacy Principle 5.
Commerce Commission	C	Supports option C. Data validation for all domain name registrations and verification for high risk domain name registrations. Together with requirement for a geographical presence, considers a data validation requirement would strongly discourage the establishment or purchase of domains for an illegal purpose. Registrants would have to be NZ based and use their own contact details. Would also bring NZ policies into line with the Australian model where a person’s identity validated before they can use a domain. Current ‘reactive’ model is not sufficient to address domain name registration abuse. Relies on both the conduct being detected and the party detecting it to have the wherewithal to pass the information on to the Domain Name Commissioner. Complaints submitter receives only a fraction of the non-compliance that goes on in NZ markets. In June 2020 submitter referred 9 .nz domain names to DNCL. Most were registered overseas. Domain Names were cancelled by DNCL. Domains may not have been registered in the first place with a robust data validation model, preventing harm to consumers.
MarkMonitor	C	Supports option C. Would however like to see the approach adopted by Nominet incorporated into this, especially the registrar status process where a registrar can achieve a “trusted” status. Would reduce the volume of identified domains. Would also like to see the approach where trusted registrars are able to validate registrant details online via a portal.

DNCL		Supports any measures to improve the data accuracy of registrant personal information in the .nz register. Majority of registrants do provide accurate registrant details. Randomness samples of the register and domain validation checks finds only a small percentage of cases where the information is not complete, up to date and accurate.
OFLC	C	Supports Option C. Strongest to help to prevent harm. Would however be the most resource intensive to implement and maintain. Option C feels like a good future focused option that, if implemented right, allows for change as the nature of use changes (with respect to ‘high risk’ definitions). Minimum the submitter would support is Option B – with the ability to move to data verification where a risk or concern was identified. With either option, new operational policies or process will need to be developed. Will likely also need to be good stakeholder engagement to ensure the best possible set of guidelines is developed and able to be maintained.
Ben Bradshaw		Submitter has used outdated details in domain registrations for years with no consequence because does not want personal address published online for easy access by anyone with access to a WHOIS lookup tool. Use a valid email address so I can be contacted in cases of a dispute. If DNCL wants to encourage people to give correct personal information, would strongly urge DNCL to make most registration details private, with the exception of contact email address/phone number and set up a system which would allow limited access to this information for abuse reports which tracks access.

Issue seven: Grace periods and domain tasting

- Option A: The current situation
- Option B: Removal of grace periods
- Option C: Adopt different policies towards new registration and renewal grace periods

Submitter		Summary of Submission
Blacknight	A	Supports a modified option A. If the concern is around “tasting” then consider a percentage based limit to the add grace period (AGP). For example if this was set at 10% of the registrar’s new adds per month then the registrar (and registrants) would still be able to deal with various issues such

		as human error or credit card fraud but this would limit the number of AGP deletes and thus avoid mass tasting.
Jay Daley	A	Supports option A. There is no evidence that any of this is even noticeable let alone a problem.
1st Domains	A	Supports option A. Would like to see evidence of abuse before the current situation was materially changed. Is not aware of any registrars that allow registration and cancellation of a domain name during the grace period as a productised service. However, this has been an issue with some Registrars in the gTLD space. Submitter has a policy of non-refundable transactions but in practice if a Registrant has made a typo, or renewed the incorrect domain name and it is within the 5 day grace period, will usually accommodate a request to resolve the situation and reverse the transaction. Does not see this option being abused or used unnecessarily and it provides a mechanism to rectify issues and provide a better customer experience for .nz over gTLDs that we offer. As a reseller for gTLDs, submitter cannot offer the same flexibility to refund customers who opt for gTLD names.
MarkMonitor	A	Supports option A. Does not support domain tasting by registrants but does support and actively uses registration grace periods and so would like these to be retained.
Berend de Boer	A	Supports option A.
Liverton Security	A	Supports option A. Removal of the grace period has the potential to create more problems which outweighs the risk of misuse of the grace period.
DNCL	A	Recommends retaining the current grace period of 5 days. There are legitimate reasons why individuals might need to use the grace periods (e.g. misspelt domain names) and it might cause significant burden if the period is removed.
Ben Bradshaw	(A)	Given Options Report states “There is no evidence that grace periods are being abused by malicious registrants in the .nz space”, queries whether there is a need for change.

Anonymous - prior work in domain names	C	Supports option C. Second choice A. As the current situation does not require registrars to refund registration fees to their customers, has not heard of domain tasting happening in New Zealand. Option C provides protection for customers who have difficulties with a renewal.
Jannat Maqbool	C	Supports option C. Enables a level of flexibility.
Hein Frauendorf	C	Supports option C. There is a need to reduce the attack surface and this seems to be the best tradeoff.
CERT NZ	C	Supports option C. Option A is beneficial to bad actors and therefore is against.
MEGA	C	Supports Option C. This would be an improvement on the current situation by still permitting registrants to rectify failed renewal payments but closing the door on the potential for using grace periods to avoid domain name registration costs when using a .nz domain name for malicious activities like phishing.
OFLC	C	Supports option C. Strongest option to prevent misuse and harm. May however bring limitations this may bring registrants. Considers the initial engagement process should be reviewed at the outset of registration to mitigate the risk that registrants make errors etc. Could strengthen option A with updated policy and in line with the implementation of an acceptable use guide or policy (as noted in previous sections).

Issue eight: Misleading, deceptive, and offensive domain names

- Option A: The current situation
- Option B: Introduce a 'reserved and restricted names' policy

Submitter		Summary of Submission
Jay Daley	A	Supports option A. Cannot tell if a domain name is a misleading or deceptive registration until

		you have seen it in use. All the registry sees is a domain name made up of letters, number and hyphens. It is rarely possible to correctly impute any meaning to that collection of characters until it is somehow used and that usage observed. What the first-come-first-served principle means is “wait until that usage is observed before making any decision on the legitimacy of that registration”. From that comes a set of implications that raise this into a guiding principle.
1st Domains	A	Supports option A. No evidence to suggest there is a problem. Otherwise you have to presume certain words are intended for abuse. Covid19 related domains are an example. Some overseas registrars blocked covid domain pre-emptively. DNCL took a monitored approach and reportedly did not suspend a single covid19 domain name. Hundreds of domain names using covid19 for the greater good were registered.
Anonymous - prior work in domain names	A	Supports option A. An automatic scanning of names for strings would lead to absurd situations like the banning of shitakemushrooms.com. See https://en.wikipedia.org/wiki/Scunthorpe_problem. Cannot see how Option B’s banning “offensive” terms would “Help make the .nz domain space more trusted and secure”. Ban would need to be vetted by humans who were raised in NZ to ensure that NZ cultural norms were respected. Unverified reports that Facebook routinely bans adverts by gay dating sites because they choose to outsource advert vetting to countries where being gay is illegal. Would be intolerable for domain registrations in NZ to be banned because of systematic bigotry in the vetting process.
MEGA	A	Supports option A. The current system operates effectively. Trying to introduce a ‘reserved and restricted names’ policy is unlikely to provide any significant improvement. Will also introduce another level of complexity and potential controversy around the registration process.
DNCL	A	Supports option A. Mixed opinions on creating an extended prohibited domain names list. Challenges when it comes to extending a domain name prohibition list: 1. Current prohibited list does not contain a complete scope of prohibited domain names (such as Ombudsman, which is prohibited by the Ombudsmen (Protection of Name) Amendment Act 2020. 2. Not clear how to draw the line on where the restriction should end. Are many words, phrases, acronyms and abbreviation that might potentially be restricted.

		3. Reserved list needs to be precise. Many of the words restricted are ambiguous as to whether they are restricted as a standalone word or as a composite word. InternetNZ has previously used a prohibited list between 2002 and 2003, which was abandoned.
David Farrar	(A)	See earlier comments on why this was done away with 19 years ago.
Blacknight	B	Supports option B, with a variation. Huge issues with any registry adopting a policy that refers to something so subjective as “offensive”. Offensive names are highly subjective and should be avoided. However having a reserved / restricted policy can make sense if adopted carefully.
MarkMonitor	B	Supports reserved list, however as a registrar, would need to have an active policy and process to remove domain names from this list where possible.
Liverton Security	B	InternetNZ has an obligation on behalf of New Zealanders to manage the .nz domain name space, including implementing and applying a reserved and restricted name policy.
Jannat Maqbool	B	Supports option B, aligns with other guidelines and what we want to see leveraging the domain
Hein Frauendorf	B	Supports option B.
CERT NZ	B	Supports option B, with careful policy considerations to balance commercial and security interests
OFLC	B	Supports option B. Provides the greatest protections. Would however mean a significant compliance/additional work requirement. Supports the list of words or phrases (phrases are important to consider) being developed and/or maintained through an external advisory group that includes industry, InternetNZ and suitable representatives such as the Chief Censor perhaps. Approach may mitigate the risk that the list is overly strict and provide some public assurance. Could also balance the freedom of expression requirements with harm mitigation – as well as reducing the overhead for InternetNZ.
Ben Bradshaw	Other	Alternative option: introduce a series of names which trigger a review after registration. Will always be innocuous combinations of characters that fall foul of filtering systems, like Pen

		Island. Retaining first come first served with a flag for domains that might be an issue to the DNCL would strike a balance. Given DNS can take 24-72 hours to propogate there is lead in time to review.
Arran Hunt		Options Report mentions someone claiming a domain, that another may have registered, based on a trademark. Trademark in itself is not the sole right to use that mark but the right to use it in a certain industry or area. More than one trademark may exist for the same term. Even without a trademark, someone may still be legally using a term in another industry and not fall foul of a trademark, and may have greater rights to it in their industry. They should have a right to that domain if they were the one to register is first. Perhaps a rule could be established for people who are cybersquatting, to encourage the use of domains, but it would need to be clearly worded. The use of what may appear to be a misspelled trademark may in itself be trademarkable, if in another industry where there is no clear confusion to consumers. Again, this needs to be clearly worded otherwise valid attempted registrants would be restricted from registering domain names they should be allowed to use.

Issue nine: Ensuring security best practice across the .nz domain name system

- Option A: The current situation: Registry has no levers to monitor or improve registrar security
- Option B: Require all registrars to adhere to minimum security standards
- Option C: Incentivise or mandate security features or practices

Submitter		Summary of Submission
Berend de Boer	A	Prefers option A. Not convinced of a problem. Note that I'm in favour of only those physically operating in NZ to allow access to .nz domain, so that will also help here.
MEGA	A	Supports option A. The Registry has no levers to monitor or improve registrar security. Supports the current situation until there is greater agreement and implementation internationally on minimum security standards for registrars.

		Imposing and monitoring compliance with mandatory security standards would be costly and time intensive. Would likely lead to increased costs being passed onto registrants, thereby reducing the accessibility and affordability of the .nz domain. Would also discriminate against smaller and new entrant registrars, who would be unlikely to have the same financial resources as larger registrars to implement. Could discourage new registrars from entering the industry, having the follow-on effect of reducing competition and increasing prices charged to registrants. Ever-increasing rate at which advances in technology occur, mandatory security requirements would also have to be constantly reviewed and updated to ensure they continued to provide the required standard of protection against current threats. Would lead to continual further costs and investment of time being required by DNCL as well as registrars.
Jay Daley	B/C	Supports combination of Option B and C. DNSSEC should not be optional and should attract a small discount for each DNSSEC domain a registrar has. Main issue against appears to be the cost to the registrar but if a registrar cannot afford the cost of operating securely then they should not be a registrar.
MarkMonitor	B	Supports option B
Liverton Security	B	Supports Option B. Many industries have requirements on matters such as privacy and security. Appropriate for domain name providers to comply with security standards. Change needs to be managed carefully e.g. communicate requirements clearly and give registrars plenty of time to modify systems. No opinion on incentives. Notes Option B and C deal with mandating and incentivizing which are two separate matters. This may affect the interpretation of results.
Michael Homer	B	Supports option B. Only one with realistic likelihood of improving the situation, with phased introduction to make it practical.
Ben Bradshaw	B	Slow and steady improvement is desirable.
OFLC	B/C	Supports Option B or C. Should be some level of base requirement for security to protect the .nz domain.
Blacknight	B/C	Supports combination of B and C. Reasonable that registrars are technically capable of operating securely. However, the baseline of this would need to be set. Adding incentives for other security

		features etc., makes it more attractive for registrars to adopt.
1st Domains	B/ C	Supports option B, with some of Option C. Should be a mandated minimum set of security standards prescribed by InternetNZ and adopted by Registrars. If there are additional security features beyond the minimum as part of the service offering like DNSSEC, registrars could be incentivised to implement and adopt.
Jannat Maqbool	C	Supports option C. This is fundamental
Hein Frauendorf	C	Supports option C
CERT NZ	C	Supports option C. Option B “should” be the minimum.
Dreamscape Networks	C	Supports option B or C. Option C would have greater impact to maintain a competitive environment whilst achieving the other goals and principles stated.
Anonymous - prior work in domain names	C	Supports option C split into two: ‘C: Incentivise ...’ and ‘D: Mandate ...’. With this change, supports alternative option D. Protecting registrants should be a high priority & allowing a domain name to be hijacked could severely impact on a business. If it is a mistake by the registrant, c’est la vie, but it would be intolerable for it to be because of slackness by registrars.
DNCL		Both options (B and C) would lead to an improvement in security. Concerned with option C. Clarification needed. Option suggests that the registry should step in and incentivise/mandate security features or practices. Doing so raises a concern as the registry might have to compete with the registrar in offering security services to the registrant. If not the intention, then the policy should clarify that.

Issue ten: Technology specific approach

- Option A: The current situation
- Option B: A ‘technology neutral’ approach to policy drafting replaces the current prescriptive approach

Submitter		Summary of Submission
Jay Daley	A	Supports option A. Technology does not change that often that the policy cannot be amended to match. Does not seem to be any evidence that this is a problem.
1st Domains	A	Supports option A. Technologies would likely be referenced under the operational guidelines which by their nature should be specific and would be expected to be reviewed and re-written more frequently anyway. Domain name technology is not changing at any great pace.
Anonymous - prior work in domain names	A	Supports option A. Instincts tend to support option B, except that if there is no list of suitable technologies, registrars may engage in unethical practices and hide behind their decision by claiming it is “more secure”. Current policies require that UDAIs are only valid for 30 days. Before this came into effect a registrar decided it would quietly change them every time a domain name was renewed or altered thus invalidating a registrant’s list of domains and UDAIs. If there was a dispute they therefore could impede the registrant’s attempt to move to a different registrar.
MEGA	A	Supports option A. Appropriate to specify specific security products like DNSSEC which play such a fundamental role in the operation of the .nz domain. The specificity may however limit the adoption of new technologies. Given that any such new technologies would play such a key role in the operation of the .nz domain, it is appropriate that the adoption of them should first require some degree of further industry wide consultation.
Ben Bradshaw	A	Supports option A. Important to specify in some detail what the requirements are when dealing with technical requirements. DNSSEC a set of requirements not a “product” as stated in Report.
OFLC	B	Supports option B. Provides for future proofing. May however mean that there is more work required internally for DNCL/InternetNZ to ensure that these policies are clearly operationally implemented according to the current technology stack.

MarkMonitor	B	Supports option B
Jannat Maqbool	B	Supports option B. More inclusive
Hein Frauendorf	B	Supports option B
Dreamscape Networks	B	Supports option B but encourages further work in this area. One possibility is a separate set of guidelines and expectations which can be adapted as technology continues to advance.
Blacknight	Other	Supports a more nuanced approach in how the policy is drafted. Would allow for specific technology to be referenced but not preclude newer technologies.
Anna Pendergrast	Other	Supports additional tech-specific operational guidance in instances where it might be needed.

Conflicted names

Issue eleven: Self conflicted names

- Option A: The current situation - the Registry continues to allow self
- Option B: Provide a deadline for the registrant to resolve the conflict themselves to avoid release of domain names.

Issue twelve: Other conflicted names

- Option A: The current situation
- Option B: Provide a deadline for all registrants to come to an agreement
- Option C: InternetNZ develops a criteria for prioritising registrants' right to a .nz name

Submitter	Self	Other	Summary of Submission
DNCL	A	A	Supports option A. Number of domain names in the conflict set has been steadily decreasing these past few years. Now a very small number. Those in the conflict set may be candidates for participants in submitter's pilot of a new online negotiation service as part of trialing new processes under its existing dispute resolution service. Submitter intends to contact those in the conflict set and invite them to participate in the pilot to try and negotiate online the resolution of their conflict.
David Farrar	(A)	(A)	Supports the submission by DNCL on the issue.
Ben Bradshaw	A	A	Self-Conflicted: Option A. If a user has declined to register the self-conflicted domain name, possibly to save money, then any change will look like DNCL attempting to get more money from the registrant. Does not fit with the goal of making it more accessible. Other conflicted: Option A. Submitter has a conflicted domain where a company has

			the .co.nz and submitter has the .net.nz. Fair arrangement if both of them want it then neither of them will have it. If it had been available when launched, submitter would have made an attempt to get it but as the other registrant is a company they could probably out-bid submitter with no benefit for themselves except domain coverage. You don’t change a .co.nz to a .nz when all your infrastructure is already set up. You redirect the domain to your current primary domain and move on with paying $20-30/year as the cost of being online. Companies in NZ have registered .xxx domains with their company name just to protect their image. Prefers the options are presented in a way that focuses on the benefit to the registrants rather than the goal of getting more .nz domains registered and therefore more revenue. The idea that “Growth in use of .nz domain names [is] facilitated” by changing the status quo ignores that there would be no new registrants, just more domains per registrant.
Dreamscape Networks	B	A	Supports option B for self-conflicted names. Supports option A for other conflicted names. Does not believe there should be favoring or priority of rights, particularly at this stage with arguably retrospective action.
Blacknight	B	B	Supports option B for both. Should have been handled better when the policy was changed to allow for the registrations. It now just needs to be cleaned up.
Michael Homer	B	B	Supports option B for both. These artificial conflicts have no benefit. Remaining unregistered 2LDs should go to open registration. Terminal case should be an auction among conflictees or general release if no conflict participant wants to register the name. Creates a resolution and removes the concept of conflicted names. Creating a prohibited names list is no improvement over the current situation. Failing that, option A, the status quo, presents no major problem and conflicts will likely lapse over time. Option C seems to have unworkable issues in formulating the priority list.
Edwin Hermann	B	B	Supports option B for both. Pointless for self-conflicted domains to continue to remain conflicted. Option B is a pragmatic solution to the problem. Also does not

			favour one registrant over another. Disadvantage identified in the Options Report that registrants do not understand the issues and how to resolve them can easily be addressed by communicating with these registrants.
1st Domains	B	C	Supports option B for self-conflicted names. Easy and straight forward approach. Supports option C for other conflicted names, with priority going to the registrant that has held the third level name for the longest. Does not support that .co.nz has priority or a more legitimate claim. Would seem unfair.
Anonymous - prior work in domain names	A	C	Supports option A for self conflicted domains. Enough time has gone by. They should either pay the $20 / year to register the name or let someone else have it. Supports option C for other conflicted names. Would prefer option 1 (earlier or earliest registration). Another option would be to make the conflicted name a moderated 2ld (one of the original options when registrations at the second level was introduced.
MarkMonitor		C	Has no preference for resolving self-conflict. Supports option C for the other conflicted names. Where there is a longer standing third level the holder of that domain should be given priority. Or where there is a registered valid TM the holder should be given priority. Proposes an additional option for other conflicted domains. If the deadline does not result in the interested party being awarded the domain but the domain is released to the public, should be a time limit for a response from interested parties, and domains are awarded after that time directly to the interested party.
Jannat Maqbool	B	C	
OFLC		C	Supports option C. Recommends that an 'exceptions policy/process' be developed to provide flexibility for cases that don't fit the criteria.

Responses to web video ‘conflicted domain names’

These submitters responded to the video on how to resolve conflicted domain names (other, not self conflicts).

Submitter		Comments
Carrie	C	First dibs should go to whomever registered the name first. Who was first to register should also be told of anyone else wanting to use a similar name and they can obstruct it. They should also be given the right to decide if they want to continue using their current name or switch to .nz or .org.nz and the ones that are not chosen or changed from
Brockden	C	
Oliver	C	
Andrew	C	Prioritise local ownership of .nz (registrant is a citizen or company is headquartered / pays most of it's tax in NZ, for example)

Enhancing privacy across the .nz domain name system

Two Submitters made high level comments on privacy and .nz that were not related to any single issue. These are provided below.

Submitter	Summary of Submission
Office of the Privacy Commissioner	Considers that the purposes for collecting registrant data is the primary issue that should drive the Panel's consideration of privacy issues in the review. This is consistent with the approach of the Information Privacy Principles in the Privacy Act 1993. Clearly articulating the purposes for which registrant data is collected will assist in answering the discussion paper's questions. The OPC is mindful that issues such as the guiding principles being considered for the .nz domain space may influence the purposes for collecting registrant data and considering whether it should be publicly available. For example, a 'secure, trusted and safe' principle could mean that registrant data is more tightly held than currently (or conversely, that it is publicly available to provide for public scrutiny). Recommends the Panel seek further information from InternetNZ and the DNZ. Specifically, information relating to the relationship between transparency and accountability and public access to registrant data, as well as complaints or concerns raised regarding public access to registrant data. Is aware that making registrant data publicly available can create privacy risks. For example, screen scraping of WHOIS functionality can be used to create reverse lookup systems. The Panel should consider whether the benefits of public access outweigh the privacy risks presented.
Arran Hunt	Privacy is certainly an important factor. However, so is openness. In NZ, we have a culture of certain information being open. Some examples are the address details of shareholders and directors, the ownership of properties, the registered securities on people and companies, and car ownership. The default for .nz should be the same. The contact information for a domain owner should be public information. Should however be a procedure for this information to be secured. Supports it being done when either a protection order is in place, or the address details are suppressed by a court for any other purpose and for the timeframe dictated by the court. Issue re people not being aware that such details are publicly available would be better

	resolved through education, or a requirement that they are made aware of this during the registration process. Already have an issue in NZ where people seem to have a disconnect between the internet and reality, with some belief that actions online are not harmful to others. Removing their personal details will just help to reinforce this view. If registrant information was to be withheld by default, then INZ should have in place some process for that information to be accessible without the need for a court order. This would be especially important for where content associated with a domain may be causing serious emotional distress to an individual, and contact is attempting to be made to ask for the content to be brought down. Requiring a court order would just result in further harm caused, and more people willing to sit behind their keyboards causing harm, knowing that they are being protected by INZ. As to the mention of the information being made available possibly not complying with the Privacy Act (either the current or the one about to come into effect), legal advice should have been sought on this. If the personal information was given with the knowledge that it would be publicly available, then it is not a breach of the Privacy Act. As above, the same standard applies for a number of other interests that people hold. Again, education on the IRPO may help resolve the issue, although I believe that domain ownership should be public information.

Issue thirteen: Level of registrant data collected and stored

- Option A: The current situation
- Option B: Introduce different registrant profiles, requiring different levels of contact data to be collected for each.

Submitter		Summary of Submission
Dreamscape Networks	A	Supports option A. Additional complexity would not benefit any stakeholders to any great capacity and it would be challenging to manage.
Blacknight	A	Supports option A if data is published. If publication of the data remains as it is currently, then supports option B..
1st Domains	A	Supports option A. Likely fits closer with the industry standard for domain name registration. Need to ensure we do not deviate away from existing best practice and start spinning our own home-grown solutions as we move to a new Registry system with EPP. Should adopt existing practices rather than re-invent, which presents challenges to implementation down the line.
Anonymous - prior work in domain names	A	Supports option A. Before considering what information needs to be made public, you should investigate the information being collected and why you need it.
MarkMonitor	A	
MEGA	A	Supports option A. Simplicity in the current model and registrar platforms have been set up to deal with the current level of data collection. Would have to consider how to treat already existing registrants if the new system was implemented and what aspects of any new system to extend to them. Considerable issues with this, including the burden it would place on registrars to deal with such historical registrants and also what was to be done with historical registrants who refused to provide the required information or verification specified under any new system. Would be better to direct more resources into public information campaigns, making registrants aware of their rights to request the Individual Registrant Privacy Option and informing everyone what personal information is currently searchable online when they register a .nz domain.

Jannat Maqbool	B	
Ben Bradshaw	B	Prefers option B. In principle providers should only require as much information as they need to offer their service to their users. However, implementation of this would be more difficult so would prefer focus to go on the IRPO.
OFLC	B	Option B obviously provides the most protections from a privacy perspective. Option A does not feel like it is appropriate to continue as is - adding some protections in is important. At the very least – all registrants need to be made aware of the discoverability of their personal data to enable them to make informed decisions.
CERT NZ	Other	No preference for option A or B. Does support accurate information gathered (email / Tel #) in relation to contact details and who to report to (when reporting phishing, malware etc).
Office of the Privacy Commissioner	Other	Level of registrant data collected and stored should be consistent with the principles of necessity and proportionality expressed in the Privacy Act. Panel should clearly articulate purposes for which information is required and then the data elements necessary to fulfil this purpose. With respect to the options, if more information than is currently necessary is being collected, then this should be addressed with a view to collecting less. Agrees with the assessment of the options in this section. However, considers that the disadvantage the Panel has identified with option A (that more individuals' personal information publicly available) could be mitigated through the options discussed in questions 43-47 (like having the IRPO chosen option by default). Panel should consider the relationship between all of the options identified in questions 41-47.

Issue fourteen: Registrant data is made public by default

- Option A: Current situation
- Option B: The IRPO is opt out, i.e, individual registrants have the option activated by default
- Option C: All registrant contact details are withheld from query services for all individuals not in trade (no option to opt out or in)

Submitter		Summary of Submission
Anonymous - prior work in domain names	A	Supports option A. Before considering what information needs to be made public, should investigate the information being collected and why it is needed. For example, if the technical contact is to allow urgent communication with the person responsible for the domain name's DNS if it is causing problems, not clear their physical address is needed if you have email or phone information. If there is an administrative contact, not clear you also need contact information for the registrant. Individual registrants being given automatic IRPO assumes that most individual registrants will not be engaged in business or political activity through the website. Not clear that is true. Registrars should be required to prominently display the opt in option on the registration form. What data should be withheld from a DNS lookup query? All data should be withheld from a DNS lookup query except a working email address which does not need to be the actual final email address if InternetNZ wants to maintain a mail forwarding service.
MarkMonitor	A	Supports option A.
MEGA	A	Supports option A. Current system and approach are appropriate. Would be better to direct more resources into public information campaigns, making new and existing registrants aware of their rights to request the IRPO and what personal information is currently searchable online when they register for a .nz domain. Submitter frequently required to issue cease and desist requests in respect of other online websites. Usually in relation to registrants who are adopting the imagery and 'getup' of submitter's website to deceive and mislead consumers for various purposes, or

		trading under deceptively similar domain names to submitter's name for similar reasons. Would be unusual for submitter to find such a bad faith registrant operating under a .nz domain, difficult to find actionable contact details for such bad faith registrants overseas. In some circumstances it appears easier to hide a registrant's contact information. What data should be withheld from a DNS lookup query? Only physical address details should be withheld from WHOIS under the IRPO. Would provide for the physical personal safety of the registrant. Would still ensure that there were always sufficient details by which a registrant could be contacted for legitimate business purposes, like if a registrant was using a domain name in bad faith.
Dreamscape Networks	B	Supports option B. Best benefits the interests of registrants. What data should be withheld from a DNS lookup query? Name, Address, Phone Number
Jannat Maqbool	B	
CERT NZ	B	Supports option B. Promotes the safety of people interacting with commercial domain names.
Edwin Hermann	B	What data should be withheld from a DNS lookup query? Registrant name, physical address, postal address should be withheld. Ability to withhold other details like email address and phone number should be implemented as a per-domain option.
Ben Bradshaw	B	Supports option B. Supports not publicly listing the personal details of individuals by default. In the last few years we have seen the rise of personal information being online. While there is value for a few in having this information public there is value in not having it public for others. Does not consider many users who register a domain in NZ are aware that some of the PII ends up in a public register. They register with a username and password and provide the details to a website. They can only see those details by logging in and the assumption the data is only on the website is reasonable based on their other experiences. With the rise of doxxing and online bullying, DNS is one information source that can be used to identify individuals. As soon as IRPO was available, submitter activated it and will continue to use and where they are not eligible, they use out of date details.

		What data should be withheld from a DNS lookup query? Physical addresses and phone numbers Comfortable with the requirement for an email address to be displayed. Yearly emails to ensure the email is monitored would be a great thing for the DNCL to consider.
OFLC	B	Supports option B. Would however create issues for people who have legitimate cause to look up that information. Perhaps another process could be put in place to allow people with a legitimate need to seek that information through DNCL. What data should be withheld from a DNS lookup query? Full contact details for individuals – such as full address (could list city/suburb instead)
Blacknight	B/ C	Supports options B or C if there is an opt in for publication. Phrasing of B is confusing – sounds like it means data is published, yet it contradicts itself. Unless the registrant is a "legal person" the contact information should be redacted by default. What data should be withheld from a DNS lookup query? Answer depends on whether the registrant is a natural person or a legal person. Any data element that contains personally identifiable information should not be available to be mined. Should also be a difference between the port 43 service and the web based "whois".
1st Domains	C	Supports option C. Given the options to choose, cannot see why any individual would want their personal details, including email address, made publicly available. However, another option could be added and that is like Option A but IRPO must be offered during registration so that all new registrants are informed at time of Registration what their options are. Registry could be updated to include the IRPO selection value on new creates to enforce this. Option C would need a mechanism made available to contact the domain contacts. A proxy form could be used whereby you enter the domain name of the Registrant/Tech/Admin you wish to contact and it relays the email to the contact. What data should be withheld from a DNS lookup query? Would hide all the contacts from the WHOIS for individual registrants because the admin and tech is usually a duplicate of the registrant information (most registrants use buttons we make available to pre-fill these contacts with the same information during the registration process to

		make it faster). If you only hide registrant info, then there is a high chance that personal registrant details will be inadvertently publicly disclosed.
Michael Homer	C	Supports option C. Seems little reason to have a separate opt-in process on top of simply declaring the domain to be registered in trade. Individual registrants are frequently their own administrative contact so the IRPO has little impact on these registrations. This is not addressed by the options. This may be one reason the access process is little-used in those cases where it might be. While technical contact information may conceivably be required urgently, the others cannot, and should be treated equivalently. What data should be withheld from a DNS lookup query? All of them, but especially address and phone number.
DNCL		Privacy option is currently open to individuals who are not in trade. Option B and C would assume that the individual registrants are not in trade. Bold assumption. Important to note that the domain name must be used in trade. Individual can still qualify for a privacy option even if they are normally engaged in trade if their domain name is used for a personal purpose. If the privacy option was instead applied automatically to any natural person to withhold their name, phone number and address from disclosure, it would enhance the privacy rights of the individuals. Would also remove the need for submitter to audit registrars to ensure that the privacy option was only being applied to people not in significant trade. Significant trade test is ambiguous and submitter not in the best position to assess it as it involves elements of an assessment of use of a domain name. Supports removal of test and simply applying the privacy option to any natural person. If such a change were made, applying the privacy option automatically to natural persons in the .nz WHOIS may however drive up requests for access to withheld information by third parties (e.g. lawyers and law enforcement). E.g., submitter received requests in the past from a consumer protection agency for access to details of domain name holders associated with motor cars and trade. Submitter could refer the agency to the publicly available details in the WHOIS to meet the request. Consequence of this may then impact resources and processes.

		What data should be withheld from a DNS lookup query? Public consultation process between 2015-2017 suggested that the email address of a person regardless of whether the privacy option was flagged or not should still be published on the register. Was deemed justified if the registrant was engaged in trade because the normal expectation is that the trader will likely make their own information available publicly in the first place on their website.
Office of the Privacy Commissioner	Other	Making registrant data publicly available means that the domain name registry is a public register (albeit one without a statutory basis). Should be a specifically identified public interest justifying public access to the information. This public interest could form part of the purpose of collecting the information. Information made public would therefore be what is necessary for that purpose. Generally supports keeping WHOIS as a public register of registrant details. Important transparency and accountability measure. Purposes for which the information is made public could range from allowing website owners to be contacted about problems with their website, to allowing public scrutiny of who is operating a website (similar to the companies register). Panel should discuss these and any other purposes in more detail. Wide difference between the options in this section suggest potentially different public interests could be served. E.g., option B suggests that the personally identifiable information is not that useful for transparency and accountability purposes – while the current state suggests that personal information is important to the public interest.

Responses to the web video “.Enhancing privacy across .nz”

These submitters responded to the video about the IRPO and whether to change how it works.

Submitter		Comments
Kyle	A	As a systems engineer iT is often handy to be able to workout who the entity is that has some mind of issue. Very hard to find contact details once whois information is hidden if services are misconfigured. Happy for there to be a middleman here to help keep parties anonymous from each other as long as information can be communicated between the parties.
Paul	A	Make the option very clear when registering a domain name. Require that all registrars or ISPs/agents clearly provide the option to keep the information private. Allow registrars and agents to make it private by default for domains they register, if appropriate for their customer base. In all cases when the domain owners' information is private, consider requiring the registrar / agent to supply suitable generic public information, including their own contact details. This keeps the owners' information private while retaining some way route to find the owner of the domain.
Garth	A	Strongly support the public option - open source website contacts protect the rights of consumers and the public and automatic privacy will hurt them. For the small number of cases where privacy is required, say to protect a vulnerable person, this could be dealt with much as the electoral roll caters for limited anonymity. Strongly strongly recommend default set to public.
Matt	A	Treat online structures the same as corporate ones: ie, as with registering a company, the registration of a website should require a disclosure of registrant to allow for transparency and accountability.
Robert	B	

Andrew	B	
Brockden	C	Making privacy a no choice option would create an advantage over other domain names and encourage people to use .nz more. Especially if there was no additional charge for Whois privacy.

Issue fifteen: Implementation of the IRPO and access to registrant information when required

- Option A: The current situation
- Option B: Streamline the process described in clause 22 of the Operations and Procedures policy and make it more user friendly for requests to access ‘Withheld Data’
- Option C: The creation of a form that allows people to communicate with a registrant without requiring the registrant’s email address

Submitter		Summary of Submission
Anonymous - prior work in domain names	A	Supports option A. If its intent is to protect people’s addresses it seems to be working.
Jannat Maqbool	B/C	Supports a mix of B and C.
Blacknight	B/C	Supports a combination of B and C. Situations where releasing the data is important for LEA or others but this is not a binary choice. Should also allow for a “contact” option.
Ben Bradshaw	B/C	Supports option B and C. Option C is likely to be a good first point of contact for legitimate queries and Option B can follow. Would prefer both options to require a user to login so that contact requests can be audited. If Option C ends up being abused then domains could be restricted to just Option B.
OFLC	B/C	Supports option B or option C dependent on which option is selected for IRPO.

MarkMonitor	C	Supports option C. Communication can be sent to the registrant directly. However, there should be an “option B” process and procedure where the withheld data can be requested if option C has been unsuccessful.
Dreamscape Networks	C	Supports option c. Arguable as to whether you could set up a forwarding service to allow easier use and contact, such as domainname.nz@irpo.org.nz or similar. Would obviously come with technological burden and open to potential abuse. But could serve a purpose of notifying when email addresses on file no longer resolve. Easier and simpler process. Yes it is open to abuse however I don’t believe that is unique and it can be mitigated through a range of technologies.
CERT NZ	C	
1st Domains	C	Supports option C. Was put forward when IRPO was originally implemented. Would need to be considered if registrant details were hidden by default given the volume of domains affected.
Michael Homer	C	Supports option C. If change is necessitated by updates elsewhere and otherwise option A.
Office of Privacy Commissioner	C	Supports Option C. Would allow registrants to be contacted through an online form without requiring the publication of a registrant’s details. However, additional information is needed on this issue. Need to understand why this information should be available upon request when it is not typically available, what tests are applied to any release, and how these purposes differ from those considered in questions 44 - 45 above.
MEGA	Other	Does not agree with the assessment of the options. No option offers meaningful change to the current process which is time consuming, uncertain and too heavily weighted in favour of protecting a registrant’s contact information, even if the registrant is operating in bad faith.

Opportunities to enhance .nz growth and improve market operation

Issue sixteen: The current flat wholesale fee structure limits innovation

- Option A: Flat wholesale fee, no rebates or incentives (Current situation)
- Option B: Enable variable wholesale pricing to Registrars
- Option C: Allow Registry to offer rebates to the registrant via the wholesale fee

Submitter		Summary of Submission
Anonymous - prior work in domain names	A	Supports option A. Other options seem complicated & there is no guarantee that registrars would pass the discounts on to the registrants.
MarkMonitor	A	Supports option A.
Jannat Maqbool	B	Supports option B.
1st Domains	B	Supports option B. Would offer the most flexibility. Would encourage innovation and participation in joint programs between Registry and Registrar.
Jay Daley	B	Supports option B. DNSSEC enabled names are a good example of a class of name that other ccTLDs have shown are adopted quicker if priced cheaper than non-DNSSEC enabled names.
Berend de Boer	B/C	Supports either option B or C. .nz domain names are significantly higher than .com/.org, and offer no better value. More competition needed.
Keitha Booth	B/C	Supports option B or C. Supports enabling variable wholesale pricing to Registrars.
Dreamscape Networks	C	Supports option C. No sizeable call to make any substantial changes to wholesale fee structures. But a lot of benefit in working with the registry (and general registrar) community to drive a unified message and approach in particular to support certain initiatives and engagement drives.
Blacknight	Other	Does not support any option. Over simplifying the options and in so doing making them more complicated. Registry should be able to offer incentives and rebates to registrars and to test

		different commercial methods of marketing the namespace. Three options outlined are not flexible enough to allow for that. Would make more sense to clearly state that all registrars are given equal access to marketing programs etc., as long as they are able to meet the criteria of the various promotions. Flat wholesale fee is a good baseline. Do not conflate that with offering incentives to grow market share in particular verticals and segments. You can do that without removing the flat pricing.

Issue seventeen: The scope of incentives to enhance market operation

- Option A: Do not incentivise registrars or registrants (the current situation)
- Option B: Allow registrar incentives to drive specific initiatives
- Option C: Require any incentive payment criteria to be designed to promote .nz policy goals

Submitter		Summary of Submission
Anonymous - prior work in domain names	A	Supports option A. Other options seem complicated & there is no guarantee that registrars would pass the discounts on to the registrants.
MarkMonitor	A	
Jay Daley	A	Supports option A. Incentivisation can be made to work but it is a huge undertaking to do it correctly. Too often turns into a habitual discount being offered with no measurement and no outcomes. New product launches can be enabled by variable wholesale pricing and are not dependent on incentivisation.
Berend de Boer	B	Supports option B. But sunset it, so if it doesn’t work out well, we can rethink.
1st Domains	B/C	Supports option B or C. Most of Option B would be covered under Option C, the guiding principles, such as growing NZ, openness etc. Provides good alignment to the types of

		specific initiatives that have been proposed.
Keitha Booth	B/C	Supports a combination of allowing registrar incentives to drive specific initiatives and designing incentive payment criteria to promote .nz policy goals.
Dreamscape Networks	B/C	Supports a little of both options B and C. Tangible benefits to both but cannot really be run in isolation from the other in order to achieve the principles set out.
Blacknight	B/C	Free market principles should apply. Not sure that the way this is being pigeon holed really works. A is a terrible option. B and C might be a move in the right direction, but they're restrictive.
Jannat Maqbool	C	

Issue eighteen: Empowering registrants could improve market performance

- Option A: Current situation
- Option B: InternetNZ works with registrars to establish a statement of registrant rights which the DNC monitors and registrars are accountable for by annual monitoring
- Option C: DNCL publishes expanded objective market information to better inform registrant choice eg. market share and renewal rates

Submitter		Summary of Submission
MarkMonitor	A	
1st Domains	A/B	Supports option A or B. Comes down to education in the market. Domain name is typically a gateway to another service like a web presence or email address. On Broadband and Power market analogy, broadband and power is like web hosting and email, the domain name would be similar to the power lines or the fibre connection that enables the service. Supports holding registrars to a certain level of service. Thought that was already the role of DNCL. If recurring complaints or frequent delayed or non-response to registrant requests by certain registrars, should be addressed through the provisions of the registrar agreement, perhaps introducing a Service Level Agreement for registrars. Does not support publishing expanded market information such as market share, pricing, renewal rates. Information could be taken out of context without having a full understanding of the registrar's business, service offerings and customer demographics. Large registrar is likely to have a lower renewal rate than a small boutique Registrar that offers a niche service to schools. Submitter is likely to have many more domain speculators as clients but that is not an indication that provides a lower level of service. Likewise, another registrar may offer lower priced domain names but online support only. Another may bundle a domain name as part of a wider service offering. Similarities cannot easily be drawn against other industries like power and broadband.
Dreamscape Networks	B	Supports option B. Collaborative approach between InternetNZ to both define and implement a set of standards that drive towards the goals of the industry as a whole would be an

		optimal result.
Blacknight	B/C	Supports options B and C together.
Anonymous - prior work in domain names	Other	Does not support any option. Considers another approach where DNCL establishes a statement of registrants' rights which is emailed to each unique registrant on initial registration and annually thereafter. Should be to each unique registrant to reduce email to people with a large number of domain names. Option C is not mutually exclusive with any of the other options. Would like to see it implemented regardless.
Jay Daley	Other	Unable to respond without much more thought.
Keitha Booth	Other	Supports InternetNZ working with registrars to establish a statement of registrant rights which the DNC monitors holds registrars accountable by annual monitoring. Supports the Registry collecting & communicating market information including customer segments, activity/utilisation & product use for industry to better understand & develop the .nz market. Openness and transparency would illustrate InternetNZ's own values and public good ethos.

Issue nineteen: Improving the regulation of Resellers could enhance market operation

- Option A: The current situation
- Option B: Establish a two-tier registrar system which incorporates resellers
- Option C: Reduce the $3,000+GST registrar establishment fee for existing resellers as part of the proposed two-tier registrar system

Submitter		Summary of Submission
MarkMonitor	A	
Dreamscape Networks	A	Does not agree with the statement "It is difficult to hold resellers accountable, and to ensure they minimise inappropriate or harmful activities." Is a challenge but not material if managed

		with appropriate process and procedures. Supports option A. Does not see any issues or concerns in managing the current scenario. Two-tiered approach would add a significant level of complexity for all stakeholders involved for little benefit. Revenues could be negatively impacted but does not consider that is material. Particularly in consideration of the challenges of supporting and managing resellers as they grow and attempt to navigate between the tiers.
Anonymous - prior work in domain names	A	Already a requirement section 3.15 of Roles And Responsibilities “Be responsible for all actions of any person or organisation acting as a reseller through the authorised registrar. Resellers are required to meet the same obligations and standards as registrars in their dealings with domain names and registrants” (www.dnc.org.nz/content//roles_and_responsibilities_2.2.pdf). i.e. registrars are responsible for ensuring that DNCL policies are implemented for domain name registrations for which they are the registrar of record. If registrars choose to permit resellers they are responsible for the activities of the reseller and need to ensure that the DNCL policies are implemented. There are guides and sample contracts they can use to ensure that resellers act appropriately. https://www.dnc.org.nz/registrars/resellers https://www.dnc.org.nz/sites/default/files/2016-02/Final_Reseller.pdf https://dnc.org.nz/node/1634 Supports option A. Preamble seems to say, without evidence, that this is not happening. “The Panel believes the overall lack of regulation of resellers creates an inability to hold them to account for inappropriate or harmful activities. This situation creates frustration for registrars, registrants and the registry.” Potential option A+: option A plus existing policies are enforced by the registrars and DNCL. A+ as described in submitter’s answer to 57. Even a fee far lower than the proposed $3000 establishment fee would make it uneconomic for submitter to continue reseller activities. Large number of technically competent people likely to manage a domain or two for friends or relatives. Attempting to make low-level “technical” reselling more difficult to use might lower the reliability and possibly integrity of .nz. Would need to have a reasonably high number of customers and/or domains being cared for before requiring a formal registration of resellers.

DNCL	A	Supports option A. Regulation should be enforced from the registrar level.
Jay Daley	B	Supports option B. Other ccTLDs have done this very successfully. No reasons we should not.
CERT NZ	B	Supports option B. Two tier system will help build a better framework which will promote trust and security within the system.
1st Domains	C	Requires some further thought into why resellers would choose to identify as a reseller and what's in it for them to do so. Not clear what controls or incentives would be put in place to convert and be regulated under a reseller agreement. Should talk with auDA to understand what of their reseller process works and what does not. Optional in their space to get a Reseller ID that tags the domain names you manage on behalf of Registrants. https://www.auda.org.au/industry-information/resellers/ Supports modified version of option C. Similar to the auDA approach, could be designated Tier 1 Registrars that you can officially resell through. Could put an official reseller agreement in place between the Tier 1 Registrar and the reseller. Tier 1 Registrar would be responsible for the conduct of the reseller. Tier 1 Registrar would operate a platform that meets .nz minimum standards and be approved by InternetNZ. Would be standardised preferential pricing offered to official resellers via the Tier 1 Registrar. If the reseller later wished to become a registrar, could potentially have any establishment fee reduced or waived given their acceptable and competent operating history as a reseller. Model would reduce the burden on InternetNZ for oversight and compliance of many small operators. Would also ensure that resellers are using platforms that meet minimum standards and best practices mandated by the Registry.
Blacknight	Other	Framing of "reseller" is far too broad. Look at how it has been done elsewhere. Clearer framing of the actual problem that needs to be solved would be helpful. Reviewing the costs for becoming accredited is probably a good idea. Should however be a reasonable barrier to entry in line with the ethos of .nz being stable and secure. Other registries have offered the option for the reseller field to be optional and for the registrar to set this in the whois or RDAP output (both Nominet and EURid support this). Does not support sxpanding contractual relations to include resellers. Would cause problems as would be competing against your own channel.

Issue twenty: The Registry's role in market activity

- Option A: No requirement on scope of registrar offering. Registry may not sell/market directly to customers (The current situation)
- Option B: The Registry defines minimum service/feature set all registrars must provide. The Registry may not sell/market directly to registrants. The Registry incentivises registrars to provide services it provides under agreed rules
- Option C: No requirement on scope of registrar offering. The Registry may sell/market directly to registrants under strict controls.

Submitter		Summary of Submission
Blacknight	A	Supports option A. While it might be a good idea about setting certain requirements on registrars eg. they need to provide customer service etc., expanding that to specify which services they offer is problematic. However if you look at offering incentives via marketing promotions then you can probably get to the same place.
Edwin Hermann	A	Supports option A.
DNCL	A	Supports maintaining the separation of relationships between the registry, the regulator, the registrant and the registrar. Critical to protecting choice and competition for registrations and among registrars and providing the necessary oversight of .nz. Clause 3.6 of .nz policy on Principles and Responsibilities restricts communication between registry and registrants, stating that the normal avenue ought to be through the authorised registrar. Exception only when the communication is for customer research and .nz marketing. Avoids usurping the functions of the registrars and intervening in commercial relationships between registrars and registrants. Options Report stated the intention to ensure security best practice across the .nz domain name system and assessed the possible options to implement improvements. One of the possible changes was that the Registry takes on a more proactive role in encouraging heightened security by creating or promoting security features and mandating their

		implementation or providing incentive to encourage implementation. Evidently, the Registry is encouraged to implement these practices through the registrars. However, the option does not exclude the possibility of the Registry developing a direct channel to offer these features to the registrants directly. Doing so would broaden the instances of the registry contacting registrants. Should consider impacts on the structural separation principle and clause 3.6 of the Operations and Procedures policy.
Dreamscape Networks	B	Supports option B. Comfortable with taking this approach, if within regular consultation practices. But it may inhibit innovation around the domain name space that may not require utilisation of certain typical services and solutions.
Anonymous - prior work in domain names	B	If there were a differentiation between core registration services & add-ons it could be useful to expand the options. Concerned by the “registry lock” option. Does not recall this as part of the current .nz offerings. If implemented, could be used by a rogue registrar to block transfer of domains to another registrar by a disgruntled registrant. All registrars should offer DNSSEC and IPv6 glue records. DNCL should mandate this. Would not oppose DNCL offering paid options other than core registration and DNS security and selection functions directly to end users. One useful option would be a service that monitors and reports on any change to the registration record.
Jay Daley	B	Supports amended option B: the Registry defines minimum service/feature set all registrars must provide. Registry may not sell/market directly to registrants. Registry incentivises registrars to provide services it provides under agreed rules. Does not agree with the incentivisation as the variable wholesale pricing is sufficient. If .nz decides mandatory features through an open process rather than arbitrary decisions, no excuses for registrars not to implement them. Exactly what happens in many other industries with a wholesale/retail split.
CERT NZ	B	Supports option B. All registrars should provide the minimum feature set that includes the appropriate baseline security features. (e.g. all registrars must support DNSSEC). Issue ‘whether the registry should market to registrants’ should be discussed as a separate issue.
1st Domains	B	Registry needs a mechanism to deliver service and feature improvements to the market. Does not oppose certain features/services being mandated under a minimum feature set to grow capability within the .nz space. However, customer relationship should remain with the

		registrar/registrant to avoid conflict of interest arising and confusing lines of communication. Does not support the Registry being able to sell/market directly to registrants.
Liverton Security	B	Two separate matters here: (1) the registry selling/marketing directly to registrants (the scope of the registry’s offering); (2) a minimum service/feature set available to registrants. Need to be dealt with separately. Supports Option B. InternetNZ has an obligation to decide on the minimum service/feature set available to registrants e.g. DNSSEC, on behalf of New Zealanders. Does not believe InternetNZ should trade directly with registrants. Would conflict with its role as standard setter.
MarkMonitor	Other	No comment

Issue twenty one: Improving Registrar monitoring may enhance market operation

- Option A: The current situation
- Option B: Establish a Registrar Service Level Agreement System to enhance market operation.

Submitter		Summary of Submission
Edwin Hermann	A	Supports option A
Dreamscape Networks	B	Supports option B. Supports a consultative approach to build a framework which can be applied to drive consistency (along with enhanced reliability and security, etc).
Anonymous - prior work in domain names	B	Supports a qualified option B. Would like more detail on what is being measured.
CERT NZ	B	Would like to see cyber security aspects as part of a registrars monitoring system. (e.g. tracking levels of domains used for abuse by registrars).
1st Domains	B	Supports option B. A Service Level Agreement is lacking. Could be a useful tool to assist with the fair operation of .nz. Fair set of guidelines and minimum service standards would ensure .nz remains a high-quality offering and is a fair playing field among registrars. Would be particularly important if a 2-tier system is introduced for resellers.
Blacknight	Other	Some form of Service Level Agreement might be appropriate. ICANN model is however for registries not registrars. Not sure why it is cited as an example of anything.
Jay Daley	Other	Unable to respond without much more thought.

Issue twenty two: Greater industry data collection and publication could improve growth opportunities

- Option A: The current situation
- Option B: The Registry collects and communicates market information including customer segments, activity/utilisation and product use for industry to better understand and develop the .nz market

Submitter		Summary of Submission
Edwin Hermann	B	Supports option B.
Dreamscape Networks	B	Supports option B. Would require additional investment from InternetNZ but the data would ultimately create an enhanced environment to drive greater growth and retention.
Anonymous - prior work in domain names	B	Supports option B. Accessible information is always nice to have and sometimes useful.
CERT NZ	B	Supports option B.
1st Domains	B	Supports option B but excluding market share information and specific commercial data on Registrar operations.
Blacknight	B	Supports option B. Other registries are using data to inform their decisions as well as to assist the channel to market.
Jay Daley	B	Supports option B. Registry collects and communicates market information including customer segments, activity/utilisation and product use for industry to better understand and develop the .nz market.
Jannat Maqbool	B	Supports option B.

OFLC	B	Supports option B. Information would be useful to those working in the various factions of internet safety/regulation to understand the lay of the land, hopefully leading to better engagement and interventions. Far too often people are working from anecdotal evidence and not understanding how the markets are operating.

Issue twenty three: Second level (2LD) market opportunities

Submitter	Summary of Submission
Anonymous - prior work in domain names	Horse is well and truly bolted on this. All good names except com.nz are either registered or conflicted. To create a new 2ld would need to negotiate the purchase of the existing name from the current registrant(s). Forcibly acquiring registered names to create moderated 2lds would severely undermine the principle that ".nz be a domain space people trust and feel safe using". Names ltd.nz, inc.nz, charity.nz for registered companies, incorporated societies and registered charities would have been nice but they are gone. com.nz is currently restricted. Could be made available for registered companies with matching names similar to .com.au.
Blacknight	Not unless there is actual demand.
CERT NZ	Interested in any further discussions around additional moderated 2LD for vulnerable market segments (e.g. banks, govt). Should also be further discussion around current unmoderated 2LD's (e.g. .school.nz) as the majority of the general public believe they are.
Dreamscape Networks	Unlikely to be much demand for the majority of second level domains within the space. They add more choice and availability if most users choose not to engage with them. But they do not serve a lot of purpose. They could also add more confusion to the decision making process. Most registrars recognise this however and do not present them as an available choice anyway.
Edwin Hermann	No comment
Jannat Maqbool	Should be a way to add something to the .NZ that indicates if that website can be used data free. Needing to read information promoting websites that can be used without data is harder than just

	having a domain name extension or something that can easily identify websites that can be used without data.
Keitha Booth	Supports further work to understand any opportunities for new moderated Level 2 domains. Submitter previously managed the govt.nz domain. Was regular evidence that the public valued and had confidence in .govt.nz names. Created a strong obligation for the registrar to manage that domain at a very high standard and only accept soundly-argued applications. Very relevant now to assess whether additional moderated Level 2 domains are needed.
1st Domains	2LDs have probably had their time and any moderated domain names would be low in volume. Would be likely that InternetNZ would need to facilitate the registration of any new moderated domain names e.g operate a close Registrar for the purpose of registering moderated domain names.
UniversitiesNZ	See submission for detailed proposal on creating .edu.nz: https://drive.google.com/file/d/1dMalE6ysG1LaGgJwTptr8lp0JG2fzXgI/view?usp=sharing