Re-imagining the future of .nz

The Domain Name Commission's submission.

domain name commission nz

Table of contents

Disclaimer: Feedback is provided by the Domain Name Commissioner (DNC), the Regulator ensuring compliance with .nz policies

1. Introduction

The Commission welcomes the Review

1.1. The Domain Name Commission Limited (**DNCL** / 'the Commission') is a subsidiary of InternetNZ, appointed by InternetNZ to manage and administer the .nz domain name space. [1]

1.2. InternetNZ is a not-for-profit-organisation, that is recognised officially by the Internet Corporation for Assigned Names and Numbers (**ICANN**) as the sole authority for the administration and management of the .nz Domain Name Space.

1.3. InternetNZ is delegated to be the country-code top level domain (**ccTLD**) operator and is the stakeholder / owner to which the Commission is accountable.

1.4. The mission of the DNCL is to:

- promote public trust in our service,
- develop and monitor a competitive registrar market,
- enforce .nz policy, and
- administer an alternative dispute resolution scheme for consumers to resolve domain name disputes.

1.5. The DNCL and DNC welcome the opportunity to participate in this public consultation.

1.6. We jointly note that the way in which the Internet's policy development process is governed and developed means that there will be further opportunities to comment on these issues, and for us to influence .nz policy outputs in the future, in more detail.

2. General comments regarding the Solutions Paper

2.1. Several of the questions and options in the Solutions Paper are presented as binary choices, i.e. between one thing and another.

2.2. When you read the paper in depth, however, it becomes apparent that many of the questions, options and issues raised are interlinked.

2.3. Because of this, the enclosed response groups like and linked matters into clusters, to highlight these relationships, and a strategy for dealing with them.

2.4. In the Commission's experience of enforcing and needing to operationalise policy principles, a more nuanced and blended approach than the choices presented would be welcomed.

---

[1] InternetNZ and DNCL's relationship with Government is set out in our Memorandum of Understanding with the Ministry of Business, Innovation and Employment (MBIE)

See https://www.mbie.govt.nz/assets/0ad0efd429/internetnz-mbie-mou-dotnz.pdf

2.5. When recommending options to solve problems, we encourage the Panel to prioritise changes that have the ability to resolve more than one issue at a time.

2.6. The paper makes blanket statements, presented as delivering benefits such as 'greater trust, safety and security in .nz', but doesn't include any supporting information. As a result, it's difficult to properly assess some of the options, and whether they will deliver the stated benefits, without some explanation of the 'how' and the 'why,' as well as the 'what'.

3. Our approach

3.1. The Commission's response groups like and linked matters into clusters of questions, to highlight the relationships, and a strategy for dealing with them.

3.2. Table 1 highlights what DNCL has been able to cover in the timeframe provided for its response.

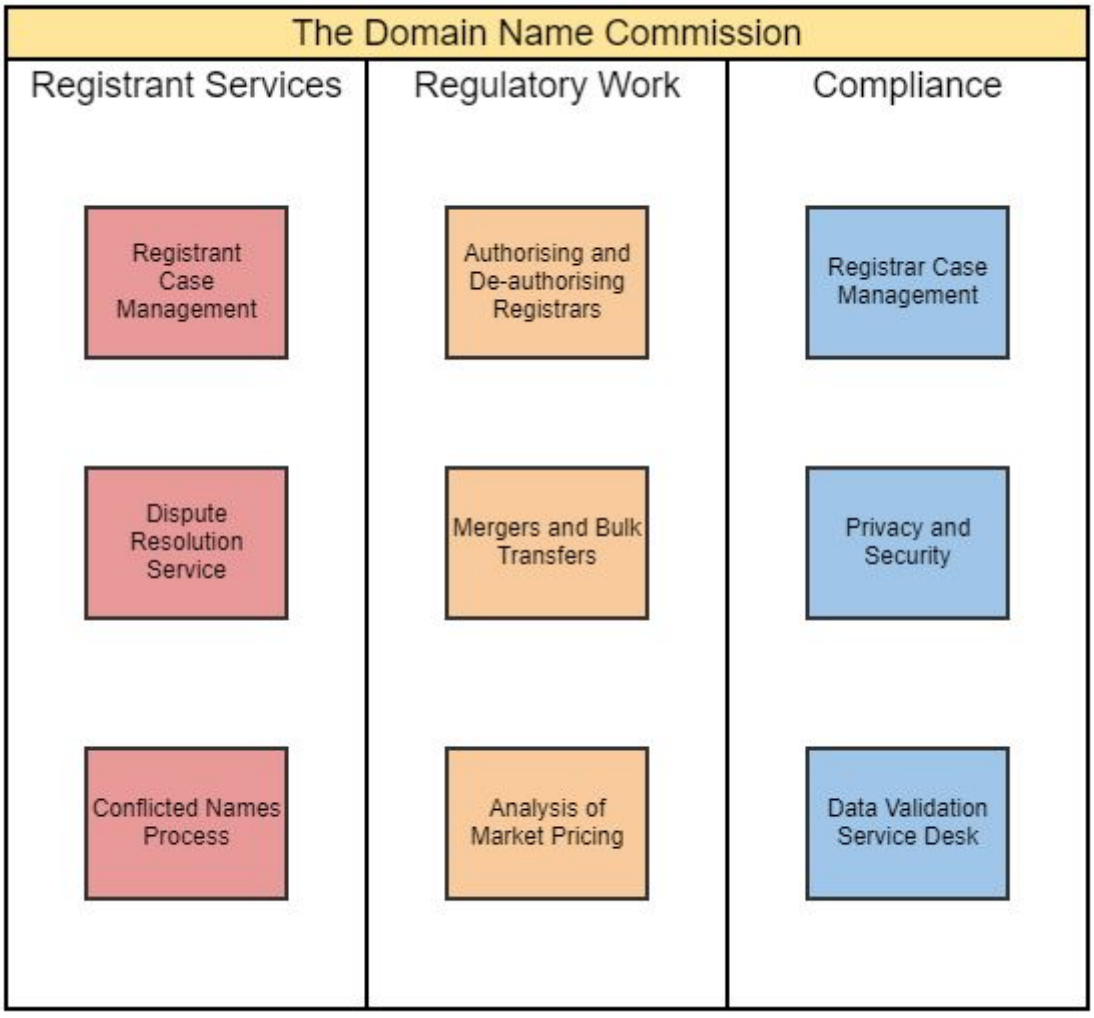
Table 1. Overview of DNCL response grouped by topic

Heading	Consultation questions
1. General comments/ Background DNCL functions	Questions 17 and 18.
2. Principle - Registrants' rights and responsibilities.	Question 12.
3. Data Accuracy	Questions 18, 28 and 30.
4. Appropriate policy architecture and structure, including difference between operational guidance and principles	Questions 1, 2, 9,15, 16 and 18.
5. Rule of law should remain, possibly described as 'obey the law'.	Question 10.
6. No concern for use and secure, trusted and safe.	Questions 3,4 and 14.
7. Open and accessible.	Questions 5, 19, 20, 21, 22 and 23.
8. Geographical restriction	Questions 22 and 23.
9. Character language exceptions	Questions 21 and 22.

10. New Zealand benefit.	Question 6 and 8.
11. First come, first served.	Question 11.
12. Market, including relationship between the registry and market and structural separation	Questions 8, 13, 51, 52, 53, 54, 55, 56, 59, 60, 61, 62, 63, 64, 65 and 66.
13. Resellers' market.	Questions 57 and 58.
14. Grace periods.	Questions 31 and 32.
15. Privacy.	Questions 41, 42, 43, 44, 45, 46 and 47.
16. Conflicted Domain Names.	Questions 39 and 40.
17. Te Reo Māori.	Question 7, 48, 49, 50.
18. IDNs and the use of emojis.	Questions 25 and 26.
19. New moderated spaces and prohibited list of domain names.	Questions 33 and 34.
20. Locks	Question 18 and 67.
21. Online harm in the DNS, registration abuse and online safety .	Questions 3,4 25, 26, 27, 28, 29, 30, 35, 36, 37 and 38.
22. Feedback specific to the Dispute Resolution Policy.	Questions 17 and 18.

4. Background - DNCL functions

Table 2. Overview of DNCL Operations



4.1. As a self-regulatory body, the DNCL complies with its own policies and contractual agreements in carrying out its day to day functions.

4.2. The DNCL:

4.2.1. is in a contractual relationship with registrars that are or wish to become authorised to operate in the .nz domain name space.

4.2.2. ensures that registrars function with the appropriate standard of technical and organisational skills and knowledge to comply with their obligations; and

4.2.3. maintains the power to investigate and ensure the compliance of registrars.

4.3. The DNCL also provides:

4.3.1. a public web based .nz query search service, (WHOIS,)[2] which is an important tool supporting DNCL functions, and other third party agencies, in their compliance and law enforcement work.

4.3.2. information and education to the general public about its services, the domain name system and domain name market, and shares information through its contact centre, website and social media presence.

4.3.3. a Dispute Resolution Service (**DRS**) when the rights of the registrants are disputed.

4.3.4. The DRS is a three stage process consisting of:

i) informal mediation (DNC covers the appointment of mediator);
ii) expert determination; and
iii) appeal to an expert panel.

4.4. The DNCL maintains a rotation of mediators and experts that it appoints to handle disputes. The decisions of the experts are collected and made publicly available.

4.5. By virtue of their sanctioning of registrants and registrars for breach of policy, The DNC (the Commissioner) performs a quasi-judicial role.

4.6. The decisions of the Commissioner are administrative and judicially reviewable.

4.7. Historically, the DNCL has not had any '*concern for use*' of a domain name, and does not assess content associated with domain names. The exception is the new interim exceptional and emergency power for domain name suspensions which has an element of consideration of use in terrorist or emergency circumstances.

5. Principle - Registrants' rights come first

Recommendation: DNCL supports this principle and agrees.

5.1. Currently, the explanation for this principle is simply: "The rights and interests of registrants are safeguarded."

5.2. The statement of a registrant-focused principle is a positive measure for registrants, registrars and the broader, locally based, .nz registered and eligible Internet community.

5.3. That being said, registrants already derive rights and responsibilities from applicable law, as well as from their contracts with their .nz authorised registrar, or reseller, in addition to .nz policies.

[2] A description of the .nz query search is available here: https://www.dnc.org.nz/whois

5.4. The way in which the .nz authorisation agreement[3] and policies treat registrants' rights and responsibilities, is to balance them with competing interests, for example, the security and stability of their registration, and that of the domain name system (DNS).

5.5. The DNCL favours retaining a statement of principle about registrants' rights and responsibilities, because it makes it clear that registrants are important in the process.

5.6. However we view this as linked to the rights arising under the law and in contract.

6. Data accuracy

Recommendation: that data accuracy of registrant personal information added to the Register, at the time of registration, be required

6.1. The DNCL supports any and all measures to improve the data accuracy of registrant personal information in the .nz register.

6.2. We note that the majority of registrants do provide accurate registrant details, and our experience taking randomised samples of the register, and performing domain validation checks, finds only a small percentage of cases in which the information is not complete, up to date and/or accurate.

6.3. Principle 8 of the Privacy Act 1993 states that an organisation must check before using personal information that it is '*...accurate, complete, relevant, up to date and not misleading*.'[4]

6.4. Current best practice, from other licensing and registration schemes, relies on obtaining accurate data at the time of registration. For example, the New Zealand Companies Office.

6.5. The actions and practices to maintain a high quality database are dynamic, and include, but may not be limited to:

- high level screening of the data provided during registration to filter out attempted false entries;
- automated checks of contact information and data provided, for example, email address[5] and phone number to see that these are working;
- cross-checks of data with official databases, for example, valid postal code, existing phone number, company/organisation number if such information is required); and

[3] Standard Registrar Authorisation Agreement available here: https://dnc.org.nz/sites/default/files/2018-05/registrar_authorisation_agreement_v5.2_4.pdf

[4] Principle 8 of the Privacy Act 1993 - see https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/accuracy-etc-of-personal-information-to-be-checked-before-use-principle-8/

[5] Checking email addresses can be difficult. Verification emails from the Commission are sometimes automatically classified as spam, or else disregarded by recipients who misunderstand their purpose.

- organised spot checks of data associated with already registered domain names; as well as
- verification of the data associated with a case or complaint.

6.6. All of these measures assist with data quality. [6]

6.7. We consider it a shared responsibility of the Registrars, the DNCL and the Registrants to maintain data quality when a domain name has an active registration.[7]

7. Appropriate policy architecture and structure

Recommendation: DNCL rejects the 'operational guidance' option and supports maintaining the policy / principle status quo

7.1. The proposal makes mention of '*principles and operational guidelines, and additional policies*' but stops short of providing clear definitions or guidance as to what is meant by 'a policy, principle, or guideline', or the next level of delegation, a rule, a process or procedure.

7.2. Problematically, there is no clear hierarchy set up to clarify the relationship between these concepts in the Solutions Paper proposals, when conventionally there would be.

7.3. We recommend consideration be given to either a standalone 'Meta Policy' that defines terminology and a hierarchy, or else an amendment to the existing policy development process (PDP Policy,) to provide clarity regarding terms and hierarchy.

7.4. Agreed definitions would be useful, and aid people in their actions and interpretations of .nz policy, as well as compliance with our rules and practices.

7.5. Because it's uncertain what form the policies will take following the proposed changes, a template, or sample policy, foreshadowing the most likely look, feel and form of what is being proposed, would be highly useful to respondents, because it provides something tangible to discuss.[8]

7.6. DNCL notes that the PDP Policy will be used to consult on the proposed changes, to allow for inputs from the local internet community, and market participants, over the definitions and governing framework. We therefore anticipate at that time there will be greater clarity around the policy architecture and structure than there is today.

---

[6] In a recent Council of Europe National Top-Level Domain Registries survey called '*Domain Suspension,'* 90% of the 21 ccTLDs surveyed, including the likes of .uk, .se, .jp, .de and .jp and New Zealand, checked data accuracy of registrant data upon receiving a complaint and through alerts.

.uk holds the registrar responsible for checking registrant's contact details. See: https://registrars.nominet.uk/uk-namespace/data-quality-policy/data-validation-on-the-whois/

[7] To ensure we have a trusted space, it's paramount that data collected from registrants is complete and validated for quality and remains valid, and current, at all times.

[8] The Irish ccTLD takes a holistic approach to policy governance and guidance and clearly differentiates between what is a policy and a guideline helping people to interpret intended meaning and application, and what is a process. See for example: https://www.iedr.ie/wp-content/uploads/2019/04/IEDR-RegistrationNaming-.IE-Namespace.pdf

8. Policy and guiding principles are not procedural

Recommendation: that the Panel note .nz guiding principles are founded on good stewardship rather than 'operational guidance'

8.1. The .nz guiding principles should lay out the stewardship responsibilities for .nz and guide those with an interest in .nz on how to act responsibly.

8.2. In 2005, the Government Advisory Committee of ICANN issued a revised set of "Principles and Guidelines for the Delegation and Administration of Country Code Top-Level Domains" whereby Guideline 4.2.1 states that:

> *The relevant government or public authority is strongly encouraged to ensure that the ccTLD is being administered in the public interest, within the framework of its national public policy and relevant laws and regulations*[9].

8.3. The guiding principles should be written with this objective in mind, and should be clear and unambiguous.

8.4. Other objectives that should be borne in mind include:

8.4.1. Retention of public trust — The public trust earned through managing existing domains must be maintained. Otherwise, trust in the DNS itself may diminish;

8.4.2. Protect DNS security and stability — An increasingly hostile environment requires coordinated, not fractured, Top-Level Domain (**TLD**) management. Stability is not the same as being dependable; and

8.4.3. If there continues to be a '*first come first served*' principle, there must be a corresponding principle that fosters an industry-based approach to an accessible, easy to understand and sustainable alternative dispute resolution process for adjudicating domain name disputes, that seeks to resolve disputes fairly, in a way that enhances peoples' trust in the stability, soundness and capacity of the DNS.

8.5. The DNCL considers that the principles are critical to the operation and actionability of .nz and the DNS and are mandatory, rather than optional in the ways that relegating them to the status of an 'operational guideline' implies they may be.

8.6. DNCL **does not support any of the existing policies being demoted** from a statement of high level principle, to the more detailed status that an 'operational guideline' implies.

8.7. Our concern is that it blurs the boundaries between the DNCL and its functions, and Internet NZ and its functions, to include the word 'operational' in these outputs.

8.8. Guidance should be confined to definitions and interpretive advice for use by ourselves, registrants, disputants, ICANN and New Zealanders in applying and enacting what is intended by .nz policy.

---

[9] See: https://gac.icann.org/principles-and-guidelines/public /principles-cctlds.pdf

9. Rule of law and the role of the law in .nz domains

Recommendation: DNCL favours retaining the '*Rule of Law is important*' as a principle and reserve power

9.1. The '.nz Policy Options Report' suggested the removal of the principle that the rule of law was important, citing a lack of "*meaningful guidance to participants in the domain name system*".[10]

9.2. Respectfully, the DNCL disagrees with that assessment.It is important to 'Obey the Law.'

9.3. The DNCL agrees that the principle is unlikely to be applied, in most cases, because of its strict conditions and powerful implications.

9.4. The fact that there is no example of the principle being invoked to undermine the Policy is not a reliable indicator of performance, since a high volume would tend to suggest that the DNC and .nz policy framework were inadequate to the task of governing the DNS.

9.5. The failure to rely on the principle is an argument in favour of keeping this principle, rather than removing it, given the message that removing it would send in the event that it was needed, and the judiciary failed to find this change in .nz policy helpful.

9.6. The purpose for the inclusion of the 'rule of law' is to place it above the operational policies for .nz, in the governance hierarchy, and acknowledge the overpowering interest of justice. It is a reserved power intended to be invoked in extraordinary cases in which following the Policy would lead to an unjust and/or perverse outcome.

9.7. The DNCL holds the opinion that it is best to retain the principle, both as a last resort and also as a warning against using the Policy for malicious reasons.

International lessons learned

9.8. We draw the Panel's attention to the Haynes' Royal Commission Report's discussion of the 'obey the law' notion as a demonstration of the importance of a similar principle.

9.9. Commissioner Kenneth Haynes' Royal Commission Report into the Australian banking sector included 'obey the law' as one of the underlying principles that should govern financial operations in Australia.[11]

9.10. He outlined the rule's importance to the general operation of the regulator, and its interactions with market participants.

9.11. His report is a salutary lesson in 'what can go wrong' in a market when people think they are above the law.

---

[10] InternetNZ (2020) Re-imagining the future of .nz. [Online] Available from https://internetnz.nz/nz-domains/nz-policies/nz-policy-review/nz-have-your-say/ [Accessed 20th July 2020].

[11] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report at 8.

9.12. The DNCL's 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.

9.13. We also consider the rule of law to be very important to developing approaches to other matters, such as domain name suspensions and cancellations. Given that this type of action should always be proportionate, and subject to the rule of law, and not contrary to any law in its execution; and

9.14. This principle is relied on by the DNCL, and referred to occasionally, when we are approached by other jurisdictions for domain name takedowns.

Application of the law to .nz

9.15. When served with requests to take down a domain, DNCL points to the need for any such request to comply with the rule of law in New Zealand, and offers that if an applicant would like an international order to be upheld, they should seek leave from the High Court of New Zealand for the order, or that outcome, to be enforced.

9.16. It is New Zealand's laws that apply to .nz, and this must be made explicit in .nz policy.

9.17. The principle should expressly remain, because it acts as a guide and assists with approaches to tackling online harm, as well as serving as a sign that New Zealand law prevails, to the extent that the law applies to .nz at all.

9.18. In broad terms, the legal framework .nz sits inside of, requires Parliament to determine what content is legal or illegal, and the courts to decide if something is in breach of the law.

9.19. If it is the case that there are stakeholders who believe that DNCL could, or should, be doing more to prevent online harm through enforcement of the law, (as the '*no concern for use*' argument in favour of removing the principle suggests), then an alternative approach would be for DNCL to work with representatives of the online safety community to develop a '**rapid domain name suspension**' process that would be open to people seeking to suspend a domain name, and authorise the DNCL to be more active in its enforcement and preparedness to uphold law-based claims, whilst providing an alternative Dispute Service that is accessible.

Rapid domain name suspension option

Recommendation: that the Panel note and consider this option

9.20. A rapid domain name suspension process could work along the lines of a criminal search warrant process, which involves

9.20.1. making an application before a District Court judge, and

9.20.2. seeking an order that can enable a rapid domain name suspension.

9.21. Such a process could be modelled on the existing processes under the 'Harmful Digital Communications Act' 2015.[12]

10. No Concern for Use and Secure, Trusted and Safe

Recommendation: retain the '*no concern for use*' principle; embed '*secure, trusted and safe*' into online harm reduction and note that further work is needed.

10.1. The DNCL supports the original principle of '*no concern for use*' as it recognises the neutral role that the DNCL and InternetNZ has in facilitating the way domain names are used. [13]

10.2. Altering the DNCL's conventional approach of *no concern for use* would mean that the DNCL takes on the role of content assessor. Prior to that happening, there would need to be an overwhelming case in favour justifying this change in direction and the form that these new interventions would take, since they would fundamentally alter DNCL's operating model and skills matrix.

10.3. At present, DNCL is an enforcer of .nz Policy, not an assessor of online content.

10.4. At a high level, it's unclear what these effective interventions might look like to know how they would or wouldn't enhance or detract from perceptions of what it means to be 'secure, trusted and safe'.

10.5. At a micro level, our evidence shows that people find the roles and responsibilities of various organisations confusing, and they struggle to know who to approach to help them access appropriate support.

10.6. It's worth stating that this new activity requires further work to establish its impacts and effects on perceptions of DNS stability and the mission and purpose of DNCL in regulating .nz.

10.7. Any new activity requires appropriate public consultation.

10.8. A timeframe, resources and impacts are worth considering and weighing up against the status quo.

10.9. Because it also risks potential infringement of freedom of speech and other civil, social, legal and human rights which contribute to the stability and security of the DNS, as well as perceptions of what is '*secure, trusted and safe*' the status quo, on balance, is more viable and preferable in the short term.

---

[12] See advice from the Ministry of Justice about the process for applying for a harmful digital communications order https://www.justice.govt.nz/courts/civil/harmful-digital-communications/applying-for-a-harmful-digital-communications-order/

[13] The only exception to this position is in terms of the existing interim clauses 11.8-11.10 which prescribe the ability to suspend a domain name in exceptional circumstances which the Commission would like to see retained. The exceptional circumstances have been triggered two times in the past 12 months, the first in relation to the Christchurch terrorist event and the second when a national state of Emergency was declared for COVID-19.

10.10. DNCL supports both principles, but recommends further work to clarify how it would fulfil this mission. Our substantive comments about online safety and a proposed approach, are elaborated on in the context of online harm minimisation elsewhere in this submission.

11. Open and accessible

Recommendation: DNCL supports the '*open and accessible*' principle.

11.1. 'Open and accessible' is an important principle and precondition to achieving an open internet. [14]

11.2. Presently, the only restrictions in place relate to:

1. moderated names;
2. whether the domain name is available; and
3. the legal age at which a person in New zealand is able to enter into lawful binding contracts (being eighteen years of age.)

11.3. Given that age is no barrier to digital competence, (and other platforms and services online have lower age limits than eighteen), .nz at some stage, may wish to reconsider whether this age restriction is appropriate, and consistent with the principle, of an open and accessible Internet and the rule of law being out of scope, since its selection has been based on the age at which an person is able to enter into binding legal contracts.

11.4. A younger age would be consistent with the principle of '*no concern for use'*, and the proposed removal of references to the rule of law.

12. Geographical restriction to New Zealand

Recommendation: DNCL does not support the geographical restriction approach

12.1. This restriction is at odds with the proposal for an open and accessible cited above.

12.2. Consistent with our earlier statements, the DNCL sees no reason for geographical limits serving as a barrier to .nz domain name registration. We support the status quo[15].

12.3. An important feature of the .nz domain name system is the liberalisation of rules with registration which make it possible for anyone in the world who is eligible to register a .nz domain name.

---

[14] Transparency and accountability - See: https://policyreview.info/articles/analysis/crucial-and-contested-global-public-good-principles-and-goals-global-internet

[15] In 2017 CENTR's Legal survey, involving 35 ccTLDs '*Localisation (local presence) requirements for registrants*' found that in most cases (66%)f registries **do not impose** any local presence requirements on registrants.

Local presence requirements for registrants exist at country level for .ca, .ie, .jp, .no, .sk and .tr..

12.4. With few exceptions[16] .nz is an unrestricted regime.

12.5. Our eligibility requirements are simple:

- be a natural person over the age of 18 years; and/ or
- a properly constituted company.

12.6. The DNCL recognises the 'tug and pull' relationship between two opposing views:

12.6.1. on the one hand, liberalisation of the rules to promote global domain name registrations and, on the other hand,

12.6.2. protecting the rights of New Zealand based consumers and businesses.

12.7. Our experience of having .nz available to everyone has shown that consumer protections and safeguards haven't been overlooked.

12.8. Protections have applied where and when they're needed, or required. For example, regardless of where you are in the world, registrants must meet the requirement to have complete and accurate registration details, and be contactable at those registration details.

12.9. If we were to restrict the registry to New Zealand persons and companies only, the existing .nz domain names that were registered by foreign entities would not be affected for quite some years to come.

12.10. As an issue of consistency with legal principle, and prospective exposure, the change cannot apply retrospectively. That is simply not good regulation or policy making.

12.11. Such a radical change would result in the .nz domain space being occupied by both NZ-connected domain names, and non-NZ-connected domain names, for as long as ten more years - the outer limit of a domain name registration period.

12.12. It is inconsistent with the principles of trust, certainty, good stewardship and stability that are so important to our decision making.

13. Character/Language Options

Recommendation: DNCL supports te reo Māori character and language options, and recommends aligning to other agencies regarding supported languages and characters.

13.1. Consistent with our shared mandate to enhance the Internet and its openness, and .nz's reputation as a '*safe, secure and trusted*' place, DNCL supports an extension of current language options to include te reo Māori to:

13.1.1. reflect New Zealand's two official languages; and

13.1.2. honour community expectations that our practices be inclusive and respectful of local conditions, needs and preferences.

13.2. However, we consider that the policy and procedure governing which characters are permitted or not permitted should align to the languages accepted by the NZ Passports

[16] If you want to register in a moderated space, and, ii) if the name is unavailable.

Office and/or the New Zealand Transport Office in the interest of smart, sustainable consistent practice.

13.3. Both agencies regularly review, assess and add new characters that are deemed to be permissible on identity documents, (passports and drivers' licenses).

13.4. Their conclusions are an objective, researched source of independent and readily available guidance, aligned to .nz interests that obviate the need for our own independent assessment of the same subject matter.

13.5. DNCL has reason to believe that the lists are updated regularly.

13.6. Where and when these agencies add characters, we can follow suit, minimising the time and effort needed to reach our own conclusions.

14. New Zealand benefit

Recommendation: further consultation is required.

14.1. The DNCL is unable to agree that a 'New Zealand benefit' test would be appropriate at this time, without closer consultation and more consideration of the detail of this proposal, and its shape and form in practice.

14.2. The test is an example of a blanket statement for which we would all like more detail concerning what is meant, and more time to develop our response.

14.3. In practical terms: what will be the test?

14.4. Will it:

14.4.1. require DNCL to assess and review services associated with a domain name - which would be a step in the direction of becoming '*concerned with use'*; or

14.4.2. be a legal requirement that we would be wise to lobby Parliament about, consistent with our position concerning:

1. who it is that has the right to determine legal or illegal content, and
2. our position on working with anti-online harm agencies; or

14.4.3. require new procedural guidelines to be created and consulted about, that identify 'other means' by which the registrant's business activities can be assessed as meeting 'the New Zealand benefit' test?

14.4.4. signal 'properly' to users, when and how and why a domain name has gained, or lost this status?

14.4.5. explain how it can be regained, (or not), and the tests, steps and remedial work needed to become or stay eligible?

14.5. At an operational level, is the benefit:

1. going to become a condition of registration and/or be self assessed, consistent with the '*first come, first serve*' principle, (and current practice);
2. will it be assessed *after* registration, by DNCL; and/or
3. continue to be tested as a benchmark for remaining registered?

14.6. Lastly, to whom or to what in New Zealand does the benefit accrue?

14.7. At a high level, a 'New Zealand benefit' principle is a deceptively simple aspiration, the way that changing the New Zealand flag is seemingly 'simple'.

14.8. The complexity of objectively assessing a 'New Zealand benefit' principle is evident from the jurisdiction of the Overseas Investment Office, which has a 'for New Zealand benefit' test.[17]

14.9. In any event, it should be noted that i) compliance costs would increase, and ii) that the test itself would pose a new, prospectively counter-productive barrier to the market.

15. First Come, First Served

Recommendation: DNCL supports the status quo

15.1. For reasons touched on in our earlier comments, '*First come, first served*' should remain.

15.2. '*First come, first serve*' has been an overarching and underlying foundation principle guiding .nz since its inception.

15.3. The principle has been fundamental to the way that .nz has historically operated; it underpins DNCL services as currently scoped, has been the basis of expert and quasi-judicial decision-making; and it dominates most of the functional areas of the DNCL.

15.4. For example: '*First come, first served*' defines the approach we use to resolve conflicted domain names, in which all registrants' rights in the 2LDs have been upheld.

15.5. The Commission's compliance efforts, (especially when it comes to the domain name audit history) rely on 'who was there first?' as a first consideration.

15.6. Previous decisions, published online, would be cast into doubt by any change to his effect, noting that stability, security and trust in .NZ and of the DNS, is something we aim to promote.

15.7. The only qualification that we offer in favour of this principle (and that we might consider helpful,) would be circumstances in which a domain name isn't able to be registered, (because it is prohibited under policy, because a new proposed principle of 'names that are contrary to New Zealand law or benefit', has been adopted).

[17] New Zealand Overseas Investment Office model test for NZ Benefit https://www.linz.govt.nz/overseas-investment/applying-for-consent-purchase-new-zealand-assets/preparing-your-application-oio/benefit-new-zealand-test

15.8. DNCL believes that a domain name should be available for registration on a '*first come, first served'* basis:

- where the domain name is not already registered in the namespace;
- when and if it is not prohibited; and
- it complies with the syntax requirements for a domain name in that namespace, (noting our existing policies of not concerning ourselves with use).

15.9. The principle helps to assert the independence of .nz, DNCL services and Internet NZ policy from other external hierarchies of rights. For example:

- a trademark owner has no better entitlement to a domain name than a business owner; and
- a registrant of a domain name in one 2LD has no greater rights to the same name in another 2LD than a third party or another 2LD registrant.

15.10. Removing this principle, without replacing it, would almost certainly require a 'root and branch review' and overhaul of DNCL services and expert decision making and may be inconsistent with ICANN requirements, in addition to threatening the stability, trust and security of the DNS because it undermines and countermands historical precedents determining registrants' rights that were otherwise fair and just.

16. Market

Recommendation: the general state of the market is healthy and competitive. No change.

16.1. The .nz domain name market is notionally competitive- judging by the lack of regulatory attention from the NZ Competition and Consumer Commission, and the range and growing number of providers and resellers, it would appear that registrants have a range of wide range of choices.

16.2. The DNCL notes that much of the discussion, centred on growing the market, is actually concerned with generating revenue.

16.3. Respectfully, DNCL does not consider there to be anything unduly restrictive that has been enacted pursuant to policy, that would adversely affect, inhibit or prohibit, revenue generation by any of the market participants.

17. Relationship between the Registry and Registrants

Recommendation: the general state of the market is healthy and competitive. No change is recommended

17.1. The DNC supports maintaining the division of labour and existing hierarchy of separation between the registry, the regulator, the registrant and the Registrar.

17.2. Separation of roles and powers, which we touched on earlier in our submission, is critical to:

1. maintaining checks and balances;
2. protecting choice;
3. assuring competition for registrations and among registrars; and
4. The 'arm's length' status needed to sustain independent and unbiased oversight of .nz.

17.3. Under the existing .nz policy on Principles and Responsibilities, cl 3.6 restricts communication between registry and registrants, stating that the normal avenue ought to be through the authorised registrar.

17.4. The exception is limited to when the purposes of the communication is for customer research and .nz marketing. This is largely to avoid usurping the functions of the registrars, and intervening in commercial relationships between Registrars and registrants.

17.5. The Options Report states that the intention is to 'ensure security best practice' across the .nz domain name system and assess the possible options to implement improvements.[18]

17.6. The report suggests, as one of the possible changes, that the Registry take 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.

17.7. Through this mechanism, the Registry is encouraged to implement these practices through the registrars.

17.8. However, the option *doesn't exclude the possibility* of the Registry developing a direct channel to offer these features to the registrants directly.

17.9. Doing this will broaden the instances of the registry contacting registrants, and consideration should be given to impacts of these changes on the structural separation principle and clause 3.6 of the Operations and Procedures policy.[19]

17.10. Resellers' Market

Recommendation: DNCL supports Registrars being held responsible for the actions of their resellers, ultimately.

17.11. The Commission has a contractual relationship with .nz authorised registrars and can more easily enforce policy compliance with registrars who are a contracted party.

17.12. The DNCL does not have an existing contractual relationship with resellers.

---

[18] .nz Policy Options Report (July 2020)

[19] When it comes to data quality and security, there are other initiatives such as scorecards, naming and transparency reporting which can be implemented.

For example, see SIDN's Registrar scorecard aiming for data quality: https://www.sidn.nl/en/news-and-blogs/registrar-scorecard-aiming-for-quality

17.13. For the clarification of doubt, the provisions under .nz policy should make it apparent that resellers are held to the same .nz requirements of .nz registrars.

17.14. We support this amendment.

18. Grace period

Recommendation: retain the status quo, noting the further work required

18.1. The DNCL suggests that the five day grace period, and current approach, is fit for purpose, and should remain unchanged.

18.2. It is important the Panel note that currently:

18.2.1. a particular domain name can only be cancelled once within a one month period; and that

18.2.2. if a name is cancelled and re-registered, then it cannot be cancelled for a second time within the five day grace period, meaning a registration fee is payable.

18.3. Prior to changing this rule, as part of due diligence and deliberation, the DNCL recommends further research be undertaken by InternetNZ on deletion rates during the grace period, to determine whether these are negligible or not.

18.4. It's worth stating that

1. it's standard consumer law and contract practice to allow 'a cooling off period';
2. having a fixed time frame provides certainty;
3. a five day cooling off period appears to work for .nz;

18.5. Examples of parties who have:

18.5.1. mistakenly misspelled their domain name, and needed to cancel it; and

18.5.2. sought a refund, and to re-register another domain name, within the five days, have been brought to our attention.

18.6. Allowing for a grace period has a positive impact on regulatory operations and agility.

18.7. The proposal is supported.

19. Privacy

Recommendation: that the Panel note DNCL resources and processes will be impacted by the proposed change

19.1. For the purposes of the Privacy Act 1993 the DNCL is considered an Agency.[20]

19.2. Consistent with the Act, the individual registrant privacy option (IRPO) has been created.

19.3. Following a two year public consultation process on the WHOIS in 2015-17,it was deemed to be necessary to continue to publish a natural person's email address in certain circumstances, regardless of whether the privacy option was flagged by the registrant, or not.

19.4. This was deemed to be justified, when or if, the registrant was engaged in trade, on the understanding that a person engaged in trade would almost certainly make their email address publicly available on their website, meeting one of the tests in the Act concerning publication[21].

19.5. Noting that it is a condition of registration of a 'dot.co' domain name that it shall be used in trade, and consistent with our view that the *'rule of law is important,' the* DNCL has adopted the definition of 'trade' found in the Fair Trading Act 1986 at clause 8.3 of its own internal compliance framework[22].

19.6. The definition of 'trade' under this Act, is extensive :[23]

> *'...trade means any trade, business, industry, profession, occupation, activity of commerce, or undertaking relating to the supply or acquisition of goods or services or to the disposition or acquisition of any interest in land.'*

19.7. The Commerce Commission also publishes a helpful summary of what would be considered being 'in trade'.[24]

19.8. The IRPO protects registrants of .nz domain names, who are ***not*** substantively engaged in 'trade' from having their personal information disclosed in the online WHOIS version of the .nz Register.

---

[20] The DNCL is also an agency with obligations under the General Data Protection Regulation. Anonymisation and pseudo-anonymization play an important role under the GDPR.

[21] See principle 11(b) under s 6 of the Privacy Act 1993

[22] DNC Operations and Procedures policy. See: https://www.dnc.org.nz/resource-library/policies/1479

[23] s. 2 Fair Trading Act 1986

[24] See https://comcom.govt.nz/business/your-obligations-as-a-business/what-is-being-in-trade.

19.9. The graph below highlights the popularity of the individual registrant privacy option (IRPO) amongst .nz domain name registrants in 2019 and 2020, respectively.

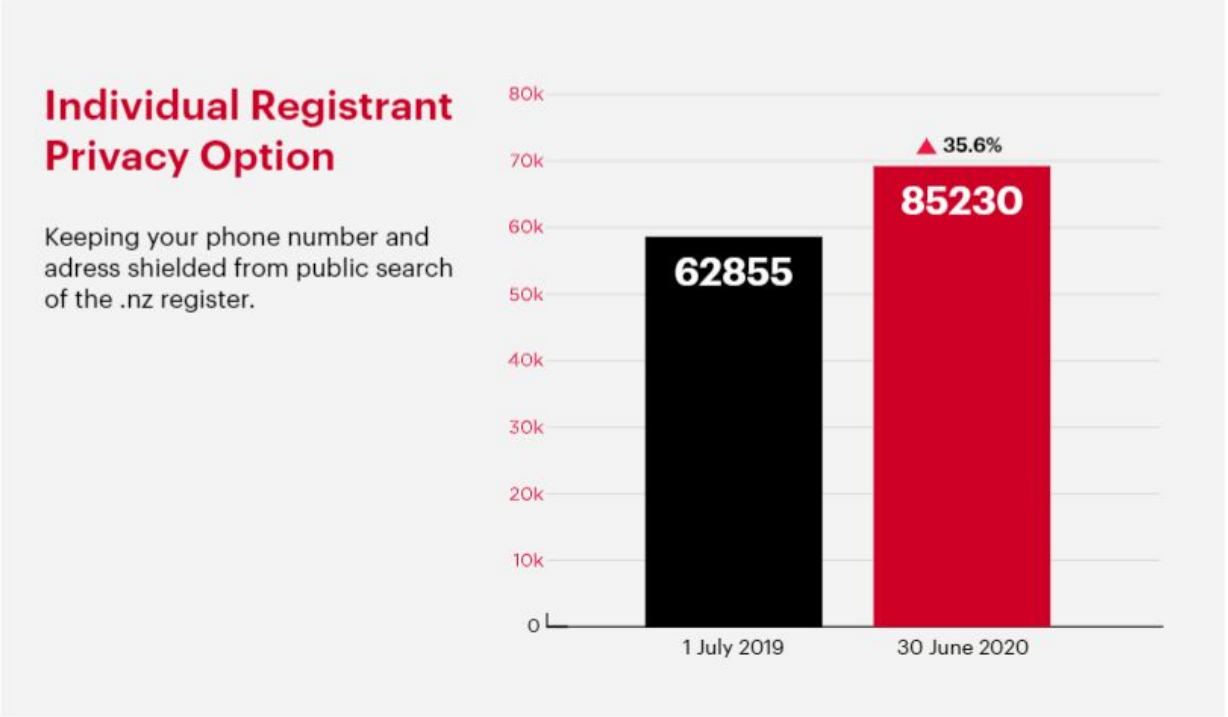


Figure 1: Current IRPO registration levels

19.10. The DNCL assumes that many individuals who register a 'dot.co' and/or, who use the domain name for the purposes of selling goods or services do not qualify for the WHOIS privacy option.

19.11. The individual can still qualify for a privacy option, as long as their domain name is used for a personal purpose.

19.12. The DNCL agrees that if the individual privacy option were to automatically apply to any natural person, withholding their name, phone number and address from publication it would enhance privacy.

19.13. The impact of the proposed change would remove the need for the DNCL to audit Registrars to ensure that the privacy option was only being applied to people not in significant trade.

19.14. As it stands, the DNCL considers the 'significant trade' test too ambiguous.

19.15. The DNCL is not in the best position to adjudicate the 'significant trade' test, since it involves elements of judgment, assessment and *concern for use* of a domain name, that have previously not been a hallmark of its activities and are best reserved to the other, specialist agencies and/or registrant self-assessment.

19.16. The DNCL proposes replacing the test of 'significant trade' with an 'eligible privacy option' to be applied to any natural person, noting that the effect of such a change on DNCL would be to drive up requests for access to withheld information by third parties

(for example lawyers and law enforcement) and impact on operations and stakeholder timeframes.

19.17. DNCL has previously fielded requests, from a consumer protection agency, for access to details of domain name holders associated with motor cars and trade.

19.18. At the time, the DNCL was able to refer the agency to the publicly available details in the WHOIS to meet the terms of the request.

19.19. DNCL resources and processes will be affected by the proposed change[25].

20. Conflicted Domain Names

Recommendation: retain status quo pending outcomes of proposed pilot of dispute resolution services

20.1. The DNCL notes that the number of domain names in the conflict set has been steadily decreasing these past few years.

20.2. There is now a very small number of domain names remaining in the conflict set.

20.3. The DNCL therefore favours the status quo in the immediate term of working with registrants in the conflict set to resolve the conflict through free voluntary conflict resolution services.

20.4. We propose that those in the conflict set may be candidates for participants in the Commission's pilot of a new online negotiation service it is hosting as part of trialling new processes under our existing dispute resolution service.

20.5. The DNCL intends to outreach to those in the conflict set and invite them to participate in the pilot, with a view to negotiating the resolution of their conflict online, rather than in person or via phone.

[25] See the DNCL's latest Transparency Report, which discusses requests for access to personal information and comprehensively reports on our privacy obligations https://dnc.org.nz/node/1987

21. Te reo Māori and te Tiriti o Waitangi

Recommendation: support in principle with further work required

21.1. The DNCL notes from the Panel's issues paper that the Panel:

21.1.1. found strong support to protect te reo in the .nz space based on its stakeholder engagement, but

21.1.2. mixed feedback on whether there should be a strong connection to te Tiriti o Waitangi (the Treaty of Waitangi) and .nz.

21.2. It is the Panel's view to explore this issue further. It is the panel that considers the .nz space could enable Māori to better connect and grow businesses in ways previously unavailable. It is the panel's view that New Zealand and .nz could take the lead on this issue globally.

21.3. The DNCL therefore looks forward to the feedback from the community on this issue to inform the Panel's thinking.

22. Internationalised Domain Names (IDNs) and the use of emojis

Recommendation: the impact of any additional IDN's requires further research to understand if any changes would need to be made to the .nz Dispute Resolution Service policy.

22.1. As previously mentioned, the DNCL supports adding *characters*, where and when these are added to the approved list of characters for identity documents, such as a New Zealand passport, or New Zealand drivers' licences.

22.2. Noting that this definition is unlikely to include or extend to emojis in the near future, (unless or until symbols become widely used and commonly accepted as meeting the test for a formal identity check and used in common names) emojis would require further consideration of their implications and impacts on operations and the principles of stability, trust and 'safe' spaces.

22.3. In principle, the DNCL recognises the improvements in usability and inclusion that will result from people around the world being able to access the Internet using their local script and supports this.

22.4. However, the DNCL also notes that with regards to IDNs, the 'IDN World Report' has identified that:

1. Registrar support for IDNs; as well as
2. universal acceptance and uptake of IDNs; and
3. user awareness pose particular challenges that are ongoing and unresolved.

22.5. The acknowledged risks associated with the use of emojis in IDNs is shown below[26]:

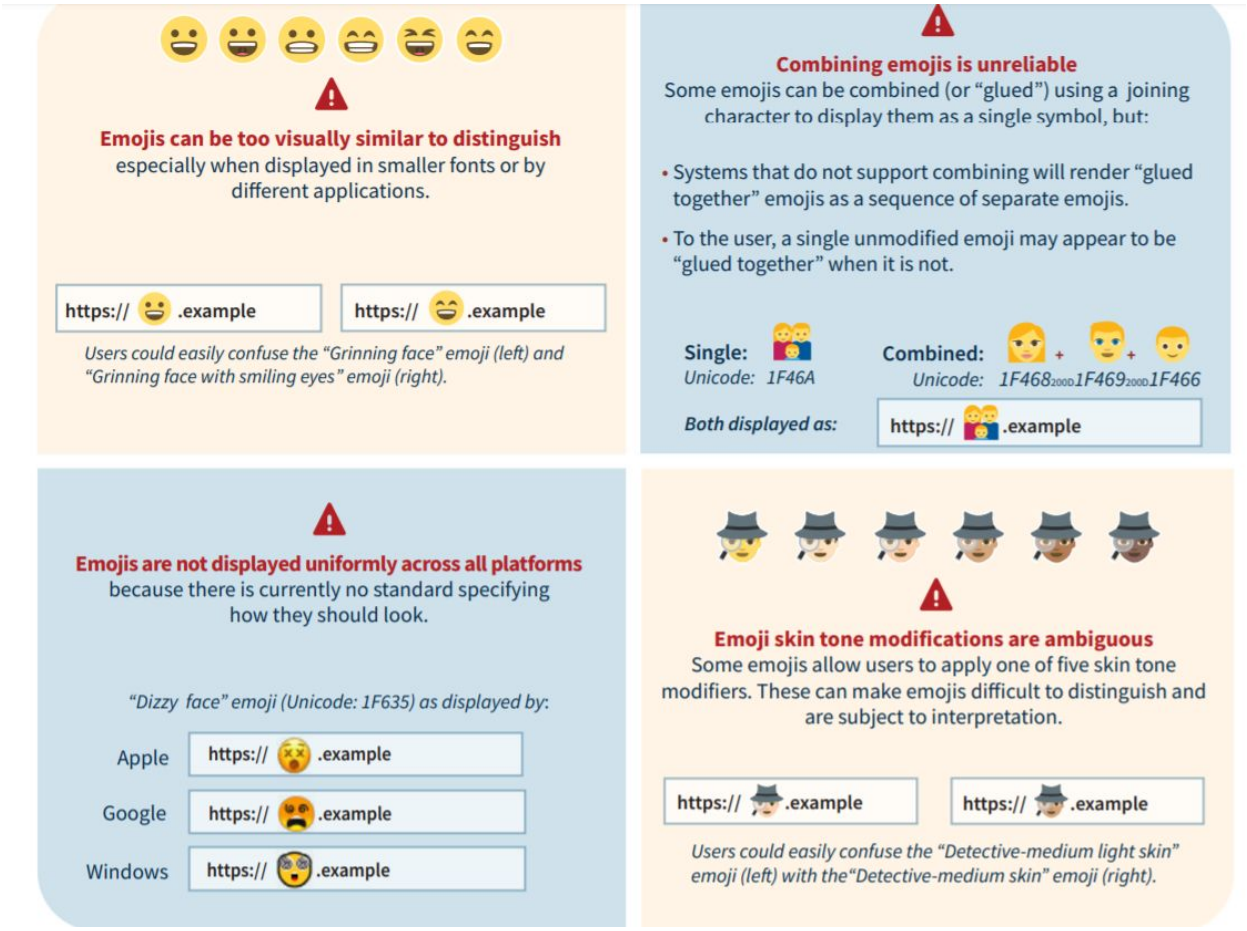


Figure 2: Excerpt from IDN World Report analysing use of emojis

22.6. To support people from around the world being able to access the Internet using their local script, the DNCL has:

1. conducted stakeholder consultations in te reo Māori;
2. supported the development of the Internationalised Domain Names infrastructure within ICANN; as well as
3. the formation of the Public Interest Registry (**PIR**) that operates four IDN TLDs (.opr, .संगठन, .机构 and .组织机构).

22.7. However, IDNs – with their use of alternative Unicode character sets, exacerbate known risks with user misidentification, caused by similarity in spelling and appearance of a URL, that in turn affect user trust and perceptions of .nz as a safe place.

22.8. It is worth reiterating that the *'no concern for use'* principle prevails, and that Parliament or else the judiciary, are the parties most suited to determining the legality or illegality of a site or its content, and by extension, emojis, consistent with the '*rule of law is important'* principle.

[26] https://www.icann.org/en/system/files/files/idn-emojis-domain-names-13feb19-en.pdf

22.9. Because te reo and other non-Latin alphabet based languages utilise alternative character representations that resolve to similar character shapes to those already in use, (including subtle accented variations such as ä, ā or ė,) their adoption increases the likelihood of conflicts and domain name disputes arising, caused by similar looking (names that visually look identical to a user).

22.10. The Solutions Paper does not discuss that most alternative scripts are already available in top level IDNs[27] and what the impacts and effects have been on the market, and on regulatory operations.

22.11. The impact of any additional IDN's on .nz requires further research to understand if any changes would need to be made to the .nz Dispute Resolution Service policy and DNCLactivity.

23. New moderated spaces and prohibited list of domain names

Recommendation: retain the status quo on moderated domain spaces. More time needed / further work on prohibited domains

23.1. DNCL supports the status quo concerning new moderated spaces being closed, and has mixed views about overseeing a prohibited domain names list.[28]

23.2. More work is needed to establish the pros and cons and consult with stakeholders noting that .nz has previously experimented with and ceased to operate a prohibited domain list.

23.3. We welcome input from the local internet community, and the Panel's examination of words, phrases, acronyms or abbreviations which should be unavailable for registration.

23.4. We note that prohibited lists impact the principle of *no concern for use* discussed earlier in our submission and query what the rationale for stopping this practice in the past may have been on the understanding that there is a lesson to be drawn from.

---

[27] Solutions Paper at 38.

[28] It appears very few ccTLDs operate prohibited lists.
We found only a handful of countries including: .fr;.au; .no; and .pt;
See: Sehttps://www.afnic.fr/en/resources/reference/charters/terms-subject-to-prior-review/
See: https://www.norid.no/en/om-domenenavn/regelverk-for-no/vedlegg-a/
See: Article 10 https://www.auda.org.au/policies/reserved-list-of-names-faq/
See: https://www.dns.pt/fotos/gca/regras_registo_.pt_en_8370975585bd74c5d0c6ee.pdf

24. New moderated second levels / .edu.nz

Recommendation: reinstate archived second level domain policy and broaden the remit of the proposal

24.1. The Commission notes the request by Universities of New Zealand for a new moderated second level .edu.nz domain name space that is not currently permissible under policy.

24.2. Should there be an opportunity for new second level domains, the DNCL would expect this opportunity to be publicly consulted on.

24.3. If the new proposed .edu.nz is the only second level to be created, this affects our policy response because it represents a lower level impact on operations.

24.4. The process for establishing a new second level domain should be consistent with the now archived 'Second Level Domains' policy'[29] in our opinion.

24.5. The process should also extend to making any existing, second level, domain name a moderated space (for example .school.nz and .ac.nz).

24.6. It is worth noting that .edu is a conflicted domain name.

24.7. Even if Universities of New Zealand preferred this namespace was reserved for its use, that's not currently permissible under .nz policies.

24.8. It's foreseeable that many namespaces proposed by stakeholders contemplating a second level, would involve conflicted domain names, which would in turn create policy dilemmas, impacting on the operations and scope of the Commission and the trust, stability and certainty of the DNS and .nz.

25. Challenges with prohibited names

Recommendation: that the Panel note this advice

25.1. The DNCL has identified numerous challenges that arise concerning reserved and prohibited domain names.

25.2. They are:

25.2.1. **Scope**: The current prohibited list contains words or phrases defined under .nz policy. The list does **not** include any legislation which may prohibit the use of words, abbreviations, acronyms or phrases. For example, in March 2020 the Ombudsman (Protection of Name) Amendment Act 2020 received Royal assent which protects the name 'Ombudsman'.

[29] https://www.dnc.org.nz/content/second_level_domains_2.6.pdf

25.2.2. **Completeness:** A cursory search of the New Zealand legal information database has identified the potential for many words, phrases, acronyms and abbreviations which may be restricted where it is unclear if such a restriction would apply online to a domain name. Where should one draw the line?

25.2.3. **Appropriateness**: a reserved list needs to be precise. Many of the words restricted in legislation are ambiguous as to whether they are restricted as a standalone word or as a composite word.

25.3. We also note that in 2002, or 2003, InternetNZ previously managed a prohibited list, and that this practice was abandoned.[30] The reasons for this decision are worth investigating.

26. Online Harm in the DNS, Registration Abuse and Safety

Recommendation: further work required. Support in principle

26.1. Online harm is broadly defined and touches on a wide range of legal concepts – from hate speech, to slander; to intellectual property rights infringement; to harassment and stalking; and the sharing of sexually explicit imagery of children.

26.2. In some of these areas, the boundary between legal and illegal activity is complex and obscure. A proportionate and necessary analysis of the content is required to determine whether it is legal or not.

26.3. While the DNCL does not condone criminal activity it considers that due process must be followed and decisions ought to be made by appropriate assessors of content, be it police, other regulators, online platforms, specific content regulators and/or judicial bodies so that this already crowded field doesn't become more crowded, and the principle of *no concern for use* is reinforced, as a means of capping the quasi-judicial scope of the Commissioner and ensuring that the sovereignty of NZ law is respected and upheld.[31]

26.4. It's important to note, that there are other more appropriate agencies who are better equipped to be the assessor of online harm for particular actions[32].

---

30 See some of the challenges of managing blocklists and strings in .nz here https://blog.nzrs.net.nz/automatic-similar-domains-detection-using-string-similarities/

31 See: https://internetnz.nz/blog/takedown-domain-names-rule-law-and-due-process/
This is also supported by legal advice received, which can be read at: https://dnc.org.nz/content/Take_down_domain_names_lawyers.pdf

32 DNCL co-operates with other agencies in tackling abuse, either by entering into formal arrangements, such as Memoranda of Understanding, or else the application of Principle 11 (and exceptions to the disclosure principle under the Privacy Act 1993).
See for example https://dnc.org.nz/the-commission/stakeholders

26.5. When it comes to online safety, DNCL manages, coordinates and acts on requests from a external agencies who have the mandate to collect, store and action reports of various types of abuse based on the following topics:

- Illegal gambling sites - Department of Internal Affairs (DIA) regulated;
- Child Sexual Abuse Material - DIA regulated;
- Illegal medicines and equipment and poisons - Medsafe regulated;
- Spam - DIA regulated;
- Terrorism content - Office of the Chief Censor regulated;
- Malware/Phishing - CERTNZ; and
- Unsolicited communication (SPAM) - DIA regulated.

27. What can the DNCL do?

Recommendation: that the Panel note the following advice:

27.1. Our position is that we will work with law enforcement and other appropriate entities to assist them in their enquiries.

27.2. We offer them our knowledge of the subject matter, status quo, our authority to act and process.

27.3. The DNCL will not cancel domain names at the request of those agencies.

27.4. DNCL will perform data validation checks[33] and *suspend* domain names (which is not the same as responding to a ' take down domain name' request. This distinction is important to maintain.

27.5. DNCL would prefer to be in the position of having to respond to an appropriate court order, clearly outlining the domain name at issue, and the action to be taken.

27.6. DNCL is ready to assist any party that may be seeking such a court action, to ensure that the order obtained is appropriate for DNCL to take the required action.

27.7. The Authorisation Agreement clarifies that DNCL is also prepared to take these actions on behalf of registrars, when and if they receive a request directly.

[33] See https://www.dnc.org.nz/complaints-nz/data-validation

28. What changes can be made to combat online harm?

Recommendation: the Panel note the following advice

28.1. On a more general note, as mentioned in our earlier statements, under the 'rule of law' section, the DNCL supports further work being done on a 'rapid domain name suspension' process, similar to applying for a search warrant and modelled on the process under the Harmful Digital Communications Act[34]

28.2. This is where we think we can add the most amount of value on this issue.

28.3. By creating, or else contributing to, a fast, accessible and fair suspension process that:

1. is consistent and respected;
2. helps the community suspend potentially harmful domain names that infringe on rights;
3. will impartially and fairly weigh competing interests; and
4. best meets the concerns of competing stakeholders' views.

28.4. We also note that the extent of DNCL's contribution in the prevention of online harm, depends on whether changes will be made to the principle of '*no concern for use*'.

28.5. If the principle remains as is, then the DNCL cannot consider the nature of the site that the domain name resolves at when deciding actions against the domain name.

28.6. The DNCL will be limited to only examining the procedural validity of the registration details, and leaving the substantive prevention of harm to others.

28.7. The DNCL recommends any policy making in this area be carefully weighed up and considered, and the interconnectedness of:

1. a principle (n*o concern for use)*;
2. a policy statement (domain name suspensions); and
3. corresponding action (a sanction against a registrant) be clear and well understood[35]

28.8. The DNCL's position is that wherever possible, the DNCL:

1. will not assume the role of assessment and investigation, but that it
2. is capable of contributing more to the prevention of online harm through:
    i. coordination with others;
    ii. giving effect to others legal decisions; and
    iii. developing a rapid domain name suspension, either as amendment to the Harmful Digital Communications Act or,
    iv. by other lawful means.

---

[34] See: https://www.justice.govt.nz/courts/civil/harmful-digital-communications/applying-for-a-harmful-digital-communications-order/

[35] The DNCL also notes clauses 2.4-2.8 which places obligations on Registrant's in relation to the prevention of online harm and illegal activity. '

See https://registrar.iis.se/files/Appendix_2A_Terms_and_conditions_se_eng_190930.pdf

28.9. The concept of something *'safe'* is mentioned at several points in the Solutions Paper, for example, questions three and four.

28.10. The DNCL is unsure what the safety expectation for industry, registrars, registrants, the registry and members of the public is, or would be in practice.

28.11. At a macro level, issues related to 'online safety' in the context of .nz and this paper, are unclear from the proposal.

28.12. Without a clear definition of what is specifically meant by 'safe', it's difficult to comment on what might be the most effective interventions.

28.13. We've proposed one intervention: the rapid domain name suspension process. However, there may be other ways to facilitate harm minimisation worth exploring too.

29. Locks

Recommendation: 'Locks' to include consideration of data quality locks. DNCL supports consideration in more detail.

29.1. The Panel has been asked to consider 'locks' a deterrence mechanism for preventing security risks and potential online harm.

29.2. In its broader consideration of locks we encourage the Panel to consider the merit, or otherwise, of a data quality lock.

29.3. A data quality lock is a feature that exists and is used in the .uk domain space[36].

29.4. The ability for DNCL to temporarily lock domains, whilst conducting a data validation check, would make it clearer to registrars and registrants when the DNCL is carrying out a data quality check, that the DNCL is carrying out a data quality check; what is involved, and how to get compliant in regards to the accuracy of contact information.

30. Feedback specific to the Dispute Resolution Policy

Recommendation: that the panel note the following

30.1. The .nz Dispute Resolution Service (DRS) has its own .nz policy, that has existed since 2006.

30.2. Over the last 14 years, changes of a small to medium scale have been made to the .nz DRS policy.

30.3. During June 2019, the DNCL undertook a first principles review of how disputes might be handled at the Commission. [37]

---

[36] Details about how the data quality lock is deployed and works in that space are available a:t https://registrars.nominet.uk/uk-namespace/data-quality-policy/data-quality-lock/

[37] https://dnc.org.nz/consultation/drs-review

The Domain Name Commission would like to take this opportunity to thank all of the participants who were party to the first principle review. Especially Joy Liddicoat, Ben Cain, and Time Brown

30.4. DNCL is unclear how the identified policy changes from that first principles review will be incorporated into any policy rewrite, given there appears to be no commentary in the Panel's paper on the topic of dispute resolution for .nz.

30.5. Should the end-to end review of .nz policies include an examination of the DRS, then the Commission draws the Panel's attention to the following findings from our first principles review of the DRS:

30.5.1. **Pilot an Online Dispute Resolution (ODR) component of mediation (and negotiation).**

Moving this process online would remove the need for parties to have to submit signed hard copies of the complaint, in triplicate, and for the documentation to be posted to parties in the mail, to participate.

30.5.2. **Introduce flexible processes tailored to the dispute**.

The current policy[38] is very prescriptive and allows for very little deviation from the current established procedure.

For example, while the Domain Name Commissioner can extend procedural time frames in exceptional circumstances[39], the current policy does not empower the DNC to:

- allow parties to shorten timeframes, when swift access to mediation/expert determination may be required in time-sensitive circumstances, or
- extend timeframes, where settlement is close but not quite concluded.

30.5.3. **A review of the restrictive nature of Clause 5.4 of the DRS policy**

The clause states 'that in making their decision, the Expert "shall not take into account any evidence of unfair registration or use which occurred more than three (3) years before the date of the Complaint[40].

30.5.4. **Consider the concept of a summary expert determination/preliminary injunction process**.

At times, the DRS is used to combat some sort of maliciousness within the disputed domain name.

While parties generally engage with the process according to the specific timeframe, at times, an immediate resolution (even temporary) to answer the need would be beneficial.

There are obvious natural justice principles that would need to apply in such circumstances.

38 https://dnc.org.nz/resource-library/policies/65

39 .nz Dispute Resolution Service P olicy, clause B11.1

40 See https://dnc.org.nz/sites/default/files/2019-09/DRS_Review_JLiddicoat_Final.pdf

For example: Our .uk counterpart has introduced an option for an Summary Decision[41].

If we wish to follow their example, we would need to discuss this with the current experts, as it would affect the application of the precedents that current cases have created.

30.5.5. **Triage Model** -

Parties that engaged with the review called for greater participation from the DNC in the .nz DRS process, especially during the triage stage.

While emphasis is on the DNC remaining a neutral steward of the process, the DNC could be more actively involved, for example through educating participants and providing relevant information to help guide parties. This also includes providing additional domain names that the respondent has registered that the party may wish to include in their complaint.

30.5.6. There were also **calls for the DNC to validate the registration information of participants prior to the .nz DRS**, to ensure that the registration information they have provided is verified.

This would also ensure that there is more engagement by respondents during the process, rather than not engaging with the process, and that false registration information has not been provided.

30.5.7. **No deterrence for parties not engaging in the resolution process.**

Many DRS decisions involve the respondent not putting in a right of reply.

While the current .nz DRS policy does allow the expert to consider if there have been previous complaints against a particular registrant, the complainant is still required to pay the same Expert Determination fee to receive a decision for a result that can likely be predicted.

1. How might non-participation under the DRS policy be addressed to ensure fairness for both the complainant and the respondent?
2. At least one submitter on the review stated that the expert's fee should not be paid exclusively by the complainant[42].

   For example, a respondent may choose to defend a domain name complaint purely for the purpose of causing distress and financial cost to the complainant.

30.5.8. **Edit of clause 10.3 of the Policy**. -

Decisions may contain personal information, including the contact details of the Parties, and the Parties consent to personal information being displayed in this way. - other than the parties names.

This contradicts moves elsewhere to protect privacy.

---

41 https://media.nominet.uk/wp-content/uploads/2017/10/17150434/final-proposed-DRS-policy.pdf, clause 12.1

42 See https://dnc.org.nz/sites/default/files/2019-09/DNC-SUBS%202019-09-19.pdf

The Commission would recommend that all identifying information, other than that of the parties names is not displayed.

About the NZ Domain Name Commission

We regulate the .nz domain name space – helping individuals with their .nz online presence.

We want people, businesses and communities to have a trusted and distinctively New Zealand online presence.

Our Services:

- authorising service providers to sell .nz domain names
- monitoring the health & competitiveness of the .nz market
- ensuring .nz policy compliance for domain name service providers and domain name users
- handling any enquiries relating to .nz domain names
- administering an independent Dispute Resolution Service

Want to know more?

You may have a question about the registration and management of a .nz domain name. You may have a domain name provider related enquiry, or perhaps you just want to learn more about how the .nz domain name space works.

Contact Us

Email:	info@dnc.org.nz
Post:	PO Box 11 881, Wellington 6142 NZ
Freecall	0800 101 151
Phone (Intl)	+64 4 472 1600

Resources

- Site Search
- Site Map
- Privacy Statement

DNC.org.nz

2020