MADE PUBLIC ON INTERNETNZ WEBSITE ON 2 NOVEMBER 2019

October 2019

An Initial briefing for .nz Panel from InternetNZ (Part Two)

This paper is Part Two of the initial briefing for the .nz Policy Advisory Panel. Part One was provided to the Panel in August 2019.

The paper is organised around various participants and their responsibilities in the .nz system. It identifies potential issues with the principles of the .nz policies as well as potential issues in the roles and responsibilities of market participants (.nz registry, registrars, resellers, registrants and the regulator (DNCL). We then talk about how the policies are currently organised and communicated to stakeholders.

The purpose of this paper is to be a starter for ten to help inform the Panel's work on the Issues Report.

We encourage the Panel to consider the potential issues and engage with a wide range of stakeholders to identify further issues. We then seek your advice on what you think the issues are, how big these issues are and whether changes to the .nz policies should be made to address them.

The issues identified are not a complete list. We anticipate more issues will be identified as the review progresses.

Potential issues with principles of the .nz policies

New Zealand's domain name system is regulated through a set of principles provided in the 'nz Framework Policy' and '.nz Principles and Responsibilities'. We ask the Panel to consider whether the principles set out in the package of .nz policies are sufficiently reflective of today's world, relevant laws and the objectives of the domain name space.

The principles from **the .nz Framework Policy**[1] are set out below:

- **Rule of law** - the laws of New Zealand apply and the lawful instructions of the courts and authorities made as part of due process will be complied with
- **First come first served** - any domain name can be registered if available for registration on a first come, first served basis
- **Registrant rights come first** - the rights and interests of registrants are safeguarded
- **Low barriers to entry** - entry requirements are not set higher than necessary to maintain a competitive, stable market for registrars
- **No concern for use** - the ccTLD manager is not concerned with the use of a domain name
- **Structural separation** - regulatory, registry, and registrar functions are structurally separated
- **Clear chain of relationships** - all registrants have agreements with their registrar, and all registrars with the registry and with DNCL. Where appropriate the DNCL can intervene in these relationships consistent with this policy, the .nz policies and associated agreements and contracts.

The **TLD Principles document**[2] was prepared in 2012. It was intended to be relevant to the entire range of InternetNZ engagement with the TLD environment and guide InternetNZ's work in the ICANN environment. It is not part of the .nz policy framework but is a precursor that evolved later in to the principles for the .nz Framework Policy. The document sets out seven principles. Some of these principles overlap with those principles contained in the .nz Framework Policy, including that the market should be competitive, and domain registrations should be first come, first served. Other principles of the TLD Principles document include:

[1] .nz Framework Policy, v2.0., https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf

[2] TLD Principles, https://internetnz.nz/tld-principles

- **Choice** for registrant should be maintained and expanded
- Parties to domain registrations should be on a **level playing field**
- Registrant **data should be public**
- Registry/registrar **operations within a TLD should be split**
- TLD policy should be determined by open **multi-stakeholder** processes. [3]

You may be wondering how these principles compare to those applied in other countries. .au Domain Administration Ltd (auDA) is the administrator and self-regulatory policy body for the .au ccTLD (country code top level domain).[4] Australia's anticipated equivalent to the .nz TLD Principles provides "objectives" of their regime (subject to change as being consulted on).[5] The objectives of the regime echo the .nz policies' principles, such as:

- promote **consumer protection, fair trading** and **competition**
- preserve the fundamental principles of **no proprietary rights** in a domain name, **first come, first served** and **no hierarchy of rights**.

Other objectives included are:

- it is **transparent, responsive, accountable, accessible, and efficient**
- improves the **utility** of the .au ccTLD for **all** Australians
- provides those **protections** necessary to maintain the **integrity, stability, utility** and **public confidence** in the .au ccTLD
- expresses licence terms and conditions in **objective** and not subjective terms
- implements **clear, predictable and reliable complaint processes.**

We have received feedback that it can be difficult to understand the .nz principles when they are are contained in multiple documents, rather than one place.

Further, it may be useful to test the principles to see if any are out of date. For example, the TLD Principles document provides that registrant data should be public. However, it may be appropriate in today's world to draw some clear parameters around registrant data being made public.

[3] TLD Principles, https://internetnz.nz/tld-principles
[4] auDA, https://www.auda.org.au/about-auda/
[5] auDA Licencing Rules, 17.6.19, https://www.auda.org.au/policies/index-of-published-policies/2019/auda-licensing-rules/

Questions for the Panel

We ask the Panel to consider:

- Is the purpose and intent of the existing .nz principles clear and easy to understand?
- Is the structuring of the existing principles (in more than one document) easy or difficult to follow?
- Are the existing principles prescribed in the .nz policies still appropriate for a modern ccTLD?
- Will the principles still contribute to the overarching vision and objectives of regulating in the .nz domain name space?
- If not, which .nz principles should be considered and revised, and how?

Potential issues with roles and responsibilities in the .nz domain name space

The .nz domain name system has a number of participants: the .nz registry, registrars, registrants, resellers, the regulator (DNCL) and future participants.[6] The .nz policies prescribe particular roles and responsibilities for these participants.

We think it is timely to review the various roles and responsibilities of those involved in the .nz domain name system. Below we suggest some areas for you to consider.

.nz registry

InternetNZ is the technical operator and manager of the .nz domain name space.[7] This means InternetNZ is the .nz registry.

The registry maintains the authoritative DNS infrastructure for .nz and second-level domains (2LDs) under .nz (for example, co.nz or .org.nz).

InternetNZ's obligations and responsibilities to registrars are detailed in the .nz Connection Agreement.[8] The responsibilities set out in that document are the minimum standard of behaviour required of the Registry. The .nz Connection Agreement forms part of the .nz policies.

Grace period in billing process for registrations and renewals

Currently, the .nz policies provide for a five day grace period for new registrations and renewals.[9] If a domain name is cancelled during the grace period, the registration or renewal will not be billed.[10] This grace period also

[6] For a list of authorised registrars, see https://dnc.org.nz/registrars
[7] See CENTR, "What is a ccTLD registry and what does it do?", https://eurossig.eu/eurossig/wp-content/uploads/2017/07/P_Centr_flyer_0517_web.pdf
[8] Clause 11.1 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities; the .nz Connection Agreement is available at: https://dnc.org.nz/sites/default/files/2018-05/connection_agreement_archived_v4.0.pdf
[9] Clause 13.4 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures
[10] Clause 13.5 of the .nz Operations and Procedures Policy.

allows registrants time to rectify failed payments without losing their domain name service.

Other registries have varying registration grace periods, for example:

- auDA uses a three day period[11]
- CIRA, the .ca registry for the Canadian ccTLD, uses five days.

The number of days in the grace period is important because if too short then it could affect a registrant's experience and retention rates. But, at the same, if the period is too long then it can be misused and may promote "domain name tasting".[12] A registrant can also return a name just before the five-day grace period expires and then re-register it again as soon as it becomes available ("domain name kiting").[13]

Many ccTLDs have shorter grace periods to deter domain name tasting and domain name kiting.

We are interested in whether the grace period for registration and renewal provided in the .nz policies needs to be changed.

Security issues that may impact the register

The .nz Principles and Responsibilities Policy sets out that the .nz registry will advise DNCL, and any affected registrars, in a timely manner of any security issues that may impact the integrity of the register.[14] The registry may validate any information sent to the registry to ensure the security, stability and resilience of the .nz domain name space.[15] Details of the validation checks undertaken will be documented and be made available to registrars.[16]

We ask the Panel to consider if this provision is still appropriate and if there are any amendments to make to it.

[11] See clause 3 of auDA's 'Domain Renewal, Expiry and Deletion Policy', 14.12.2018, https://www.auda.org.au/index.php/policies/index-of-published-policies/2010/2010-01/

[12] ICANN, 'Domain name tasting', https://www.icann.org/resources/pages/dt-motion-2008-05-21-en: this is where an entity registers a domain name and then tests to see if the name has sufficient traffic to provide more income than the annual registration fee. If the name is profitable, it is kept. If not it is used to return the domain at no cost.

[13] Wikipedia, https://icannwiki.org/Domain_Kiting

[14] Clause 11.4 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[15] Clause 11.5 of the .nz Principles and Responsibilities Policy.

[16] Ibid.

Communication between market participants

The .nz policies generally restrict the communication between the registry and registrants - typically, registrars only communicate with registrants and DNCL when sanctioning registrants.[17]

The registry can only communicate with registrants in accordance with .nz policies.[18] This includes seeking registrar approval before going directly to one of their customers.[19] Except as provided for by the .nz policies, neither DNCL nor the registry will interfere with the commercial relationship between registrant and registrar.[20] The registry is to only communicate with registrants for the purposes of customer research and .nz marketing in accordance with the policies.[21]

This bright line separation was developed in 2002, in the context of Domainz moving from being both registry and registrar, to the split wholesale/retail model currently in place. It was important that the nascent registrar market had confidence that the registry would not interfere in registrant/registrar commercial relationships.

However, there may now be wider instances where it is appropriate or beneficial for the registrant to talk to the registry and / or the DNCL.

Questions for the Panel

We ask the Panel to explore the following questions in relation to the role of the .nz registry:

- Whether there are any improvements to the .nz policies that can be made to ensure the second pillar of InternetNZ's strategic vision related to "security" in the .nz domain name is implemented?
- Should the grace period for registration and renewal provided in the .nz policies be changed? If so, how?
- If there are wider circumstances than the .nz policies currently allow where registrants should be able to communicate to the .nz Registry and / or DNCL?

[17] Clause 3.6 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[18] Clauses 3.6 and 11.8 of the .nz Principles and Responsibilities Policy.

[19] Ibid.

[20] Clause 3.6 of the .nz Principles and Responsibilities Policy.

[21] Ibid.

.nz registrars

Any legal entity can apply to DNCL to become an authorised .nz registrar.[22] Currently, the .nz policies provide that the entity needs to successfully complete an application form and meet its requirements and pay a fee (NZ$3,000 plus GST if applicable) to become an authorised .nz registrar.[23] If successful, DNCL and the registrar may execute the .nz Registrar Authorisation Agreement to create an "authorised Registrar".[24]

A registrar may cancel its authorisation status with two months' notice to DNCL.[25] DNCL may cancel a Registrar's authorisation status in certain circumstances (e.g. if they are in breach of their authorisation agreement or a .nz policy).[26] A registrar that cancels its authorisation must transfer the domain names under its management to another nz registrar.[27]

Relationship of registrars and registrants

Registrars register domain names on behalf of registrants.[28] As above, the .nz Principles and Responsibilities Policy provides that, registrants' dealings with respect to their domain names will be predominantly through their registrar.[29] The policy provides that, neither DNCL nor the registry will interfere with the commercial relationship between registrant and registrar except in circumstances provided in the .nz policies.[30]

Registrars and a competitive market

The .nz Principles and Responsibilities Policy currently provides that the .nz domain name space must be fair and competitive, offering real choice for registrants.[31] The barriers of entry must be as low as practicable for registrars and the regulatory environment must be operated and enforced in a fair and transparent manner.

The profile of registrars in the .nz domain name market has changed:

- in the past 24 months there has been market consolidation, for example, Central Nic's acquisition of iwantmyname, and voluntary

[22] DNCL, .nz Authorised Registrars, https://dnc.org.nz/registrars/becoming-a-registrar
[23] Clause 3.1 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures
[24] Clause 3.3 of the .nz Operations and Procedures.
[25] Clause 4.1 of the .nz Operations and Procedures.
[26] Clause 4.2 of the .nz Operations and Procedures.
[27] Clause 4.5 of the .nz Operations and Procedures.
[28] Clause 7.1 of the .nz Operations and Procedures.
[29] Clause 3.6 of the .nz Principles and Responsibilities Policy.
[30] Ibid.
[31] Clause 3.3 of the .nz Principles and Responsibilities Policy.

de-authorisations of local service providers exiting the market (e.g. Red Spider and Spark)

- the number of overseas registrars to local registrars has also been changing. Currently there are 57 New Zealand based registrars, and 33 overseas based ones.

We seek to understand if the structure and operating environment for registrars is ensuring a fair and competitive market (to ensure the principles are met). Presently the .nz policies provide that DNCL may take steps, or create initiatives, so that registrars do not unduly benefit from, or be prejudiced by, their size or by the nature of their operation including geographical location inside or outside New Zealand.[32]

Recently, an independent review by David Pickens found that the current policies on market concentration may be unduly constraining competition. The Pickens Report noted that, under the policies, DNCL does not allow mergers or acquisitions of registrars where the result would be an excessive market share held by the largest registrars.[33] Pickens recommended that the DNCL consider the merit of rescinding this element of the current policies, as competition risks appear minimal in the .nz space and are likely to decline over time.[34]

The Panel could explore the competition aspects of the existing policies and the performance of the market.

Incentivising registrars' performance

A further question that has arisen is whether certain registrars could be incentivised to enhance their performance and fulfil their responsibilities. A fundamental principle currently in the TLD Principles document is that parties to domain registrations should be on a level playing field.[35] We therefore ask the Panel to consider the natural tension between incentives and the market effects for registrars and other market participants.

[32] Clause 3.8 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[33] David Pickens, 'Final report: Domain Name Commission Limited (DNCL) Regulatory Review' p. 47, https://dnc.org.nz/sites/default/files/2019-08/Pickens%20Report%20-%20Independent%20Regulatory%20Review%202019v0.1.pdf

[34] Ibid., p. 51.

[35] TLD Principles, https://internetnz.nz/tld-principles

Questions for the Panel

We ask the panel to consider:

- Are the existing obligations on registrars in the .nz policies still fit-for-purpose and will they help to meet the principles and organisational objectives?

- Are the current provisions in the .nz policies still appropriate for the relationship between registrars and registrants, or should the provisions allow for a wider relationship with the registry and DNCL?

- Can we do more to encourage fairness and market competition? If so, how could the .nz policies better encourage competition, and who should be responsible?

- Do you consider registrars need to be more incentivised to fulfil their responsibilities, or to enhance their performance? If so, how?

Fees for domain names

The .nz policies currently provide that the registry will charge a fixed wholesale fee to registrars monthly for registrations and renewals.[36] This wholesale fee will be the same for all .nz domain names. Fees will be charged for the registration and renewal terms set by the registrar. The registry may also charge registrars for any optional .nz services that may be developed as agreed with DNCL.[37]

InternetNZ is responsible for setting the level of the wholesale fee in consultation with DNCL and the registry.[38] It is reviewed regularly and registrars' are to be advised of any changes.[39] The fee is to be set at such a level that ensures .nz remains a world class registry and promotes public good works in accordance with the objectives specified in its constitution.[40]

The TLD Principles document currently also sets out that domain name markets should be competitive.[41] It maintains that registrars should be well-regulated with TLD policy frameworks that support real competition

[36] Clauses 5.2 and 5.3 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities
[37] Clause 5.2 of the .nz Principles and Responsibilities Policy.
[38] Clause 13.3 of the .nz Principles and Responsibilities Policy.
[39] Clause 5.3 of the .nz Principles and Responsibilities Policy.
[40] Ibid.
[41] TLD Principles, p. 3, https://internetnz.nz/tld-principles

between them and equal treatment of registrars by the registry. It also provides registrars should face a uniform pricing structure from registries.

We are interested to understand whether the pricing structures are still relevant and appropriate given the state of the market.

We ask the Panel to explore if the clause stating the wholesale fee should remain the same for all .nz domain names, if there should be variable wholesale fees (for value add services, etc) and what that would look like if so.

Questions for the Panel

- Are the .nz policies on fee setting appropriate between the .nz registry and registrars, and other market participants (e.g registrars to registrants)?
- Is the right balance between pricing and product innovation and a fair market being struck in the current .nz policies?

Resellers

Resellers are businesses or organisations that provide domain name registration services to the public but are not .nz authorised registrars.[42] Resellers buy .nz domain names and ultimately manage domain name records for their registrants through a .nz authorised registrar. Resellers do not have direct access to the .nz registry.[43]

The Operations and Procedure Policy makes registrars responsible for all actions of any person or organisation acting as a reseller through the authorised registrar.[44] Resellers are required to meet the same obligations and standards as registrars in their dealings with domain names and registrants. The provision provides, *if a registrar does not offer registry services to what the DNC, in the DNC's sole discretion, may decide is the public, or any section of the public however that section is selected, then all users of the registrar's services will be resellers for the purposes of the .nz policies. "Public" can include government departments, offices or agencies. Ensure that any organisation, whether a reseller or not, working in any way through or with the registrar's systems operates in a manner consistent with the nz policies.*

[42] DNCL website, "Resellers", https://dnc.org.nz/registrars/resellers
[43] Ibid.
[44] Clause 20.1 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

DNCL currently encourages resellers to have an agreement with their .nz authorised registrar.[45] DNCL has a draft agreement available and a guide for .nz domain name resellers.[46] An agreement allows the reseller and registrar to tailor the provisions to their particular relationship. However, arguably, there is a lack of transparency if a registrar and reseller hold an agreement between themselves, rather than relying solely on provisions in the .nz policies.

One issue raised about resellers is there is a lack of transparency around their activity. Little data or information is known about the resellers in the market, how many domain names are being registered through resellers, and how they price .nz domain names.

This lack of data and transparency around resellers means that InternetNZ and DNCL may find it difficult to track the usage of resellers, and identify trends or linkages between domain misuse and resellers. It also means little visibility of market dynamics. Further, registrars may be reluctant to share this information with DNCL if it is considered commercially sensitive information.

We therefore ask the Panel to consider the role and responsibilities of resellers and if the provisions under the .nz policies are still relevant, appropriate and fit-for-purpose with current goals and objectives.

Questions for the Panel

We would like the Panel to explore:

- Is there a lack of transparency around resellers and their activities. If so, how big is the problem?
- Do the .nz policies provide sufficient clarity on the role of, and requirements for, resellers (e.g. clause 20 of the .nz Operations and Procedures)?

Registrants

A registrant is the person or organisation who purchases and registers the domain name licence.[47]

The interests of a registrant may not be sufficiently provided for in the .nz policies. We would like to test *who* should be able to be a registrant, if there

[45] DNCL website, “Resellers”, https://dnc.org.nz/registrars/resellers
[46] ‘Keeping the Customer Satisfied: a guide for .nz domain name resellers’, https://www.dnc.org.nz/sites/default/files/2016-02/Final_Reseller.pdf
[47] CENTR, “What is a ccTLD registry and what does it do?” https://eurossig.eu/eurossig/wp-content/uploads/2017/07/P_Centr_flyer_0517_web.pdf

are *improvements* to how people register a .nz domain name (including whether the current obligations on a registrant are fair and equitable and sufficiently transparent), and if the registrants' privacy is *sufficiently* protected.

Who should be able to register a .nz domain name?

Age of registrant

The .nz policies currently set out that registrants must be identifiable individuals over 18 years of age or properly constituted organisations.[48] We seek to understand if this minimum age is still considered appropriate in today's world.

18 years of age may be an appropriate minimum age to licence a .nz domain name. It is equivalent to the minimum age requirements for people being able to vote in New Zealand or drink alcohol.

Arguably, the age requirement could be lowered given the number of persons at this age who use the Internet, and who may wish to start businesses and for other purposes. However, the age could also be higher considering the responsibilities that come with licensing a .nz domain name. We seek your views.

Geographical location of registrant

The .nz policies appear to allow anyone based anywhere in the world to register a .nz domain name.[49] The policies do not explicitly state, for example, that the registrant must be a New Zealand citizen, reside in New Zealand or have a New Zealand "presence".

In the equivalent Australian policies from auDA, a person applying for a licence must have "an Australian presence".[50] There are no eligibility and domain name allocation criteria for the .au namespace other than an Australian presence.[51] We seek that you test whether the New Zealand regime needs a similar provision.

InternetNZ data shows by 30 March 2018 there were 318,639 unique registrants and, of those registrants:

A. 265,353 (83.2%) were from NZ
B. 30,549 (9.6%) were from Australia

[48] Clause 7.2 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[49] Clauses 7 of the .nz Operations and Procedures Policy.

[50] Clause 2.4.1 of auDA policies, 17.6.19, policies subject to change; https://www.auda.org.au/policies/index-of-published-policies/2019/auda-licensing-rules/

[51] Clause 2.4.3 of auDA policies, https://www.auda.org.au/policies/index-of-pu

C. 11,293 (3.5%) were from Europe
D. 3,312 (1.0%) were from Asia.

By 30 March 2019, there were 318,340 unique registrants (less than the previous year) and, of those registrants:

A. 264,808 (83.1%) were from NZ
B. 30,131 (9.4%) were from Australia
C. 10,147 (3.2%) were from Europe
D. 4,278 (1.3%) were from Asia.

This registrant data has been provided to InternetNZ by registrars. We trust the information provided is correct, however, this data has not been validated by InternetNZ. Further, we do not know how this data might vary in future (e.g. a spike in registrations from a particular region).

A New Zealand commentator argued earlier this year that registration should be limited to people with a *connection* to New Zealand so that .nz is a reliable signal of a connection with New Zealand.[52] Requiring a connection with New Zealand may increase the trustworthiness of the registry, and its reliability as a signal of New Zealand location and identity, but at the cost of being a small and less open registry.

On the other hand, if we restrict the ability to licence a .nz domain name *only* to New Zealand residents then New Zealanders living overseas or other viable licensees could lose the opportunity to register a .nz domain name with commercial or personal benefits. Further, many overseas residents already have a licence to a .nz domain name. InternetNZ also could lose commercial benefits from restricting a wider pool of potential registrants.

DNCL has been active internationally in protecting the rights of registrants in their domain name privacy rights. The Commission is protecting the rights of .nz registrants domiciled in the State of Washington by filing legal action against American-based company, Domaintools, for bulk harvesting their personal information and undermining their right to an individual registrant privacy option.[53]

Questions for the Panel

We ask the panel to consider:

- Who should have the ability to licence a .nz domain name?

[52] Susan Corbett, “How to protect our national .nz identity’ .nz online identity, 11.4.2019, https://www.newsroom.co.nz/@ideasroom/2019/04/11/530913/nz-should-follow-australias-lead-on-domains

[53] Domain Name Commission Ltd v Domaintools, LLC 18-35850 (9th Cir. 2019), https://internetnz.nz/nz-principles-and-responsibilities

- Is the minimum age requirement to licence a .nz domain name still appropriate?
- Should there be a geographical limit on someone who wishes to register a .nz domain name?

Improvements to how people register a .nz domain name

We would also like the Panel to look at the process a registrant follows to register for a .nz domain name licence, and suggest any improvements.

Currently, registrars register domain names on behalf of registrants.[54] Australia has a similar provision where a person must also register through a registrar.[55] In the .nz policies, the registrar must ensure the domain name is available, mandatory fields have been supplied, and the relevant fields have valid formats.[56]

Registrars' obligations and responsibilities are set out in the .nz Registrar Authorisation Agreement, the .nz Registrar Connection Agreement, and the .nz Registrant Agreement Core Terms and Conditions, each of which forms part of the .nz policies.[57]

The obligations and responsibilities of the registrant to the registrar are set out in the registrant's agreement with its registrar. That agreement must be consistent with the .nz Registrant Agreement Core Terms and Conditions. The responsibilities set out below are the minimum standards of behaviour required to operate in the .nz domain name space.[58]

Registrar's terms and conditions

Registrants currently agree to the terms and conditions of the registrar when registering their .nz domain name. DNCL provides a set of core terms and conditions for registrars to use.[59] DNCL's agreement provides that 'Registrars are encouraged to consider other terms in addition to the core terms and

[54] Clause 7.1 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[55] auDA, clause 2.2.1, a person must apply to a registrar for a licence and must use the Registrar's form, https://www.auda.org.au/policies/index-of-published-policies/2019/auda-licensing-rules/

[56] Clause 7.9 of the .nz Operations and Procedures Policy.

[57] Clause 8 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[58] Clause 9 of the .nz Principles and Responsibilities Policy.

[59] Domain Name Commission, .nz Registrant Agreement Core Terms and Conditions, v2.1, July 2018, https://www.dnc.org.nz/sites/default/files/2018-07/registrant_agreement_core_terms_and_conditions_2.1.pdf

they must be consistent with the terms of the .nz Registrar Authorisation Agreement'.

We ask you to consider:

- Are the provisions of the Core Agreement, and any other relevant agreements, sufficient? Do they allow registrants to be aware of their rights and responsibilities?

Privacy - collection, use and disclosure of Registrant's personal information

Collection and Use of Registrant's information

Under the current .nz Operations and Procedures policy, when registering a new domain name, the registrar is to supply the following data:

- domain name
- registrant name
- registrant contact details
- administrative contact details
- technical contact details
- billing term and
- if applicable the registrant privacy option, registrant reference, and other information.[60]

The .nz policies require registrars to disclose to registrants what information is required, why it is required and how it will be collected and stored, ensure that their registrants authorise the collection of their personal information, and collect the required information from the registrant and provide it to the register.[61]

If the registrant or potential registrant refuses to provide the required information free of the imposition of any non-disclosure or confidentiality conditions then the domain name it has nominated may not be registered.[62] Anyone with access to the information (including registrars) needs to comply with the Privacy Act.

[60] Clause 7.8 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[61] Clause 7.3 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[62] Clause 7.4 of the .nz Principles and Responsibilities Policy.

Since 2017, individual registrants who have not been in self-trade have been able to elect a privacy option.[63] Registrants are able to elect the privacy option at the time of registering the domain name or at any later time.[64] This feature enables individuals to provide the registry with accurate contact details and have certain personal details kept private at the same time.

If the privacy option is elected, and the registrant is eligible, the only contact information displayed in the results returned from a query is the name, email and country. Detailed address and phone information is withheld ("Withheld Data") and not displayed.[65]

An issue that has been raised, however, is that the registrant often must opt in to the option. This requires the registrant to know about the option, and how to request it. As at 23 April 2019 it is estimated there were 257,161 individuals who held a .nz domain name but only 35,005 had chosen to flag their domains with the privacy option.

We need to consider how privacy issues sit with the principle in the TLD Principles document (and also the other policies containing principles) that registrant data should be public.[66] The TLD Principles document requires that a free and publicly available register lookup service (such as WHOIS) be maintained, with relevant authoritative information about the registrant, registrar and DNS servers for the domain. We seek your views.

Disclosure of registrant's information

When a request is made for a registrant's Withheld Data then DNCL's default position is that it will not be disclosed.[67] A person or organisation can make a request to DNCL but they must establish a legitimate need for the disclosure of the Withheld Data.[68] DNCL will apply the Privacy Act (including the Information Privacy Principles).[69] If DNCL makes a preliminary decision to disclose the Withheld Data then it must notify the registrant with the request, the requestor's details and the reason for it before it discloses it.[70]

[63] Clause 8.1 of the .nz Operations and Procedures Policy.
[64] Clause 8.2 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures
[65] Clauses 8.1 and 21.8 of the .nz Operations and Procedures Policy.
[66] TLD Principles, https://internetnz.nz/tld-principles
[67] Clause 22.1 of the .nz Operations and Procedures Policy.
[68] Clauses 22.2 and 22.3 of the .nz Operations and Procedures Policy.
[69] Clause 22.4 of the .nz Operations and Procedures Policy.
[70] Clauses 22.13-14 of the .nz Operations and Procedures Policy.

The registrant has five working days to comment on DNCL's preliminary decision.[71] DNCL then makes a final decision as to the disclosure of the Withheld Data after considering the registrant's comments.[72]

The existing policies provide that DNCL must disclose Withheld Data where the disclosure is ordered by a court of competent jurisdiction or by any other order with the force of law. The registrant does not need to be consulted before the Withheld Data is disclosed but the registrant must be notified as soon as practicable after the disclosure (unless it would prejudice it).[73]

DNCL may enter into Memorandums of Understanding (MoUs) with certain entities that DNCL considers has a legitimate need for access to the Withheld Data.[74] These MoUs are published on DNCL's website and are regularly reviewed.[75] In 2018/2019, government agencies made one request for Withheld Data under their MoU with DNCL, and the data was not disclosed.

Additionally, recent international privacy law changes may mean that the .nz policies need to be updated.

The European Union's, General Data Protection Regulation (GDPR), came into effect in May 2018.[76] According to the European Commission, the aim of the GDPR is to protect all EU citizens and residents from privacy and data breaches.[77] It regulates the processing and holding of personal data relating to individuals in the European Union regardless of location.[78] When an individual uses personal data outside the personal sphere then the data protection law must be respected. When a data breach takes place, substantial penalties can apply. It could be said InternetNZ and DNCL have to meet GDPR requirements when they collect Europeans' personal information.

Notably, on 17 May 2018, the ICANN Board adopted the Temporary Specification for gTLD Registration Data. The Temporary Specification provides a single, unified interim model that ensures a common framework for handling registration data, including registration directory services (e.g. WHOIS). It aims to ensure the continued availability of WHOIS to the greatest

[71] Clause 22.14 of the .nz Operations and Procedures Policy.
[72] Clause 22.15 of the .nz Operations and Procedures Policy.
[73] Clauses 22.23 and 22.24 of the .nz Operations and Procedures Policy.
[74] Clause 22.25 of the .nz Operations and Procedures Policy.
[75] DNCL, 'Memorandum of Understandings', https://dnc.org.nz/irpo/mou and Clause 22.26 of the .nz Operations and Procedures Policy.
[76] Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation), 119 OJ L 32016R0679 (2016).
[77] European Commission, 'EU data protection rules', https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en
[78] Ibid.

extent possible while maintaining the security and stability of the Internet's system of unique identifiers.[79]

Based on the GDPR, amendments were made to the .nz Registrar Authorisation Agreement, the Registrant Agreement Core Terms and Conditions and the .nz Connection Agreement to secure compliance for DNCL, INZ and registrars. However, no changes were specifically made based on the GDPR to the actual .nz policy documents.

Internationally, registries are finding ways to comply with the GDPR and give registrants more privacy tools. Registrant data has been redacted in certain cases while law enforcement maintains access to all registry data. Nominet, the .uk registry, allows registrants to opt-in to have their information included in WHOIS.[80] CIRA masks individual registrant information from WHOIS. If a registrant's information is not displayed in WHOIS, then they can be contacted instead through an online message delivery form. This allows people to contact a registrant and, at the same time, CIRA can maintain registrants' anonymity.[81]

Questions for the Panel

We ask the Panel to explore if the current privacy settings in the .nz policies are modern, robust and aligned with relevant laws.

Specifically, we are interested in:

- Should the .nz policies deem more registrant information private, and how should it be treated?

- What improvements can be made to the current privacy option process under the .nz policies (if any)? Are registrants sufficiently aware of the privacy option? Should the privacy option be opt-out, rather than opt-in, which could protect more registrants by default?

- How does the privacy option and the principle "registrant data should be public" in the TLD Principles work together and do the .nz policies and principles need to be updated accordingly?

[79] ICANN, 'Data protection/privacy issues', https://www.icann.org/dataprotectionprivacy
[80] Nominet UK, https://www.nominet.uk/response-proposed-changes-uk-policy-arising-gdpr/
[81] CIRA, https://cira.ca/policy/rules-and-procedures/registration-information-access-rules-and-procedures

- Do the .nz policies need to be updated to reflect recent international privacy law changes (e.g. the GDPR requirements)?

Verification of registrants

When registering a new domain name, the registrar supplies data about the registrant (e.g. name, contact details, billing term, privacy option).[82] The registrar must ensure that the domain name is available, mandatory fields have been supplied, and the relevant fields have valid formats.[83]

In certain circumstances, where invalid registrant details are made known to DNCL, for example, third party complaints, media reports, systemic investigations, DNCL may contact the registrant to validate one or all of their contact details. Where a registrant fails to validate their details, a domain name may be suspended so no changes can be made to the domain name. Registrars are provided with a monthly list of their domain names that have been suspended for poor registrant data quality. Names are unlocked and re-released after various lengths of time depending on whether they are domains prone to registration abuse.

We seek to test with the Panel if more active monitoring of the accuracy of the registrants' data is required and, if so, how.

Internationalised Domain Names (IDNs)

Currently, the Operations and Procedure Policy only explicitly permit internationalised domain names (IDNs) in .nz domain names where the characters represented by the IDN are restricted to macrons (ā, ē, ī, ō, ū) in addition to the letters a-z, digits (0-9) and the '-' hyphen.[84]

IDNs enable people around the world to use domain names in local languages and scripts.[85] IDNs are formed using characters from different scripts, such as Arabic, Chinese, or Cyrillic. These are encoded by the Unicode standard[86] and used as allowed by relevant IDN protocols.[87] IDNs can be used in any part of a

[82] Clause 7.8 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[83] Clause 7.9 of the .nz Operations and Procedures Policy.

[84] Clause 5.6.2 of the .nz Operations and Procedures Policy.

[85] ICANN, 'Internationalised Domain Names', https://www.icann.org/resources/pages/idn-2012-02-25-en

[86] Today, most of the non-English and English documents on the Web are in Unicode http://www.unicode.org/

[87] ICANN, 'Relevant RFCs and IAB Statements', https://www.icann.org/resources/pages/rfcs-2012-02-25-en

domain name (subdomain, domain or TLD).[88]

What you see	**Encoded version stored in zone file**
māori	xn--mori-qsa
😀	xn--e28h

ICANN has instituted the IDN Program to assist in the development and promotion of a multilingual Internet using IDNs.[89] The program is primarily focused on the planning and implementation of IDN top-level domains (TLDs), including IDN country code TLDs and generic TLDs. The IDN Program also supports projects geared towards effective use of IDNs at the second-level of the Domain Name System, as guided by the community.

In Europe, in support of the European Union's commitment to linguistic diversity in cyberspace, EURid has shown a deep commitment to supporting IDNs.[90] EURid launched IDNs at the second level under .eu in 2009 supporting Latin, Greek and Cyrillic, reflecting the 24 languages of the European Union. In 2017, 41,000 IDNs were operated by EURid.[91] A steady decline of IDNs has been shown under .eu since the high point of 67,000 in 2010, with a decline of 4,000 IDNs since December 2016. Homograph attacks exploit confusion arising from similarities in certain characters between Cyrillic and Latin script.[92]

auDA, the registry for .au, has proposed allowing IDNs in their name space. They will support Chinese, Korean, Japanese, Arabic and Vietnamese.[93]

[88] Chris Larsen, 'Bad guys using internationalised domain names', https://www.symantec.com/connect/blogs/bad-guys-using-internationalized-domain-names-idns

[89] ICANN, 'Internationalised Domain Names', https://www.icann.org/resources/pages/idn-2012-02-25-en

[90] EURid, .eu IDNs World Report, https://idnworldreport.eu/2018-2/eu-idns/

[91] Ibid.

[92] Ibid.

[93] auDA, 'auDA licensing rules', see proposed clause 2.8, https://www.auda.org.au/assets/Uploads/auDA-Licensing-Rules-20190618.pdf

CIRA allows French accented characters. When a .ca domain name is registered, all variations of a domain name with these accented characters (referred to as an "administrative bundle") are reserved for the registrant and cannot be registered by anyone else.[94] The administrative bundle is not registered automatically to the registrant, but they have the option to register and use them.

In New Zealand, it is likely that the ability to register domain names with macronised characters is not widely known or understood. Many prominent websites use the non-macronised version of Māori words without having the macronised equivalent registered. There is likely a lack of awareness about how macrons work in domain names, which may enable abuse, as someone else could register the version with the macron and use it for abuse. IDNs could, for example, be used for phishing-style homographic attacks.[95] Many email systems do not support IDNs also, which could impact their adoption.

Across New Zealand, the proper use of macrons is growing (road signs that used to read Taupo now read Taupō). The same trend could be expected in domain name use. For instance, https://www.taupodc.govt.nz/ is registered as a domain name, and https://www.taupōdc.govt.nz/ is not.

There is also an issue with a lack of Universal Acceptance of IDNs across the Internet.[96] Many applications and systems were written before IDNs and gTLDs[97] proliferated, and are not compatible with new domain names. Some registrars may also not support the registration of domain names with IDN characters. This means domain names with macrons may not be able to use some software applications.

We do not know the size of the issue because InternetNZ does not hold data on the demand for IDNs from existing or potential registrants. However, this could be tested during the review's engagement phase.

Māori words as taonga

Many Māori words have cultural significance to tangata whenua, and to allow their registration for commercial use is likely considered disrespectful and may be considered out of line with Te Tiriti. Some may argue the current

[94] CIRA, 'Domains with French accented characters', https://cira.ca/ca-domains/register-your-ca/domains-french-accented-characters
[95] Chris Larsen, 'Bad guys using internationalised domain names', https://www.symantec.com/connect/blogs/bad-guys-using-internationalized-domain-names-idns
[96] Universal Acceptance, https://uasg.tech/
[97] Generic top level domains (gTLDs) are those that are not designated country codes. .com, .org, and .kiwi are examples of gTLDs.

policies do not sufficiently consider the cultural and intellectual property rights and interests of indigenous peoples.[98] It could be perceived that the first come first served principle for domain name registration is at odds with a Māori worldview.

One point of comparison is the New Zealand Trade Marks Act 2002, which bars the registration of a mark which would be offensive to a section of the community including Māori, and establishes an advisory committee to assess trade marks offensive to Māori.[99]

The panel may wish to consider whether Māori should be able to protect key terms considered taonga.

Questions for the Panel

We would like the panel to consider:

- How the policies can support the adoption of the Māori language in domain names?
- Should .nz support other IDNs beyond macrons?
- Should .nz prevent the registration of domain names that include Māori language and where the use of that name would be offensive to Māori?

Prohibited domain names list

The current policies restrict certain domain names from being registered, to avoid confusion. These include 'gov', 'government', 'com', 'edu', and 'nic' at the second level.[100] There is no procedure to add domain names to the prohibited domain names list.

Two pieces of New Zealand legislation feature "protection of names" clauses, that prohibit the registration of names related to, amongst others:

- the Māori television service[101] and

[98] Taiuru, Karaitiana. (2013) 'Indigenous Issues with new GTLD's' https://www.taiuru.maori.nz/indigenous-issues-with-new-gtlds/

[99] Trade Marks Act 2002, ss 17(1)(c) and 178, http://legislation.govt.nz/act/public/2002/0049/57.0/DLM164240.html

[100] Clause 9.1 of the Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[101] Section 11, Māori Television Service (Te Aratuku Whakaata Irirangi Māori) Act 2003, http://www.legislation.govt.nz/act/public/2003/0021/latest/whole.html#DLM194348

- the use of the word ‘ombudsman’.[102]

DNCL currently monitors the registry manually to identify any breaches of these Acts.

auDA holds a detailed list of domain names prohibited by law, and it reserves the right to place names on the prohibited list that may pose a risk to the operational stability and utility of the .au domain.[103]

CIRA, the registry for Canadian ccTLD .ca, maintains a restricted names list, that it updates at its discretion.[104]

We would like the panel to explore the merits of a restricted names process, based on a robust and transparent methodology with a right of appeal.

Outstanding conflicted domain names

Since 2014, .nz has allowed registration of .nz domain names at the second level for registrants who already held any third level equivalent. Second level domain names are the second level in the DNS hierarchy. Some second level domain spaces are moderated, either by government or by Māori, and others are unmoderated, and can be registered through any authorised register or reseller.

Moderated domain names have restricted registration criteria, and are moderated by an appointed third party.[105]

- **Unmoderated** second level domain names include: .ac.nz, .co.nz, .geek.nz, .gen.nz, .kiwi.nz, .maori.nz, .net.nz., org.nz, .school.nz

- **Moderated** second level domain names include: .govt.nz, .health.nz, .iwi.nz, .parliament.nz

No new second level domain names are to be created, since registration is now available directly at the second level.

Each registrant of the conflicted name needed to indicate by October 2017 via DNCL that either they:

[102] Section 28A, Ombudsmen Act 1975, http://www.legislation.govt.nz/act/public/1975/0009/latest/whole.html#DLM431187

[103] auDA, ‘Index of published policies’, 08.01.2019 (current), https://www.auda.org.au/policies/index-of-published-policies/2014/2014-06/

[104] Clause 3.4, CIRA, https://cira.ca/policy/rules-and-procedures/general-registration-rules

[105] See DNCL, ‘Moderated second levels’, https://www.dnc.org.nz/moderated-second-levels

- wanted the opportunity to register the equivalent name for possible registration at the second level, or
- did not want to register the equivalent name and did not want any other party to register it, or
- did not want to register the equivalent name and did not object to another registrant registering it.[106]

The policy provides that, if a registrant of a conflicted name did not indicate a preference by 18 October 2017 then that conflicted name ceased to be a conflicted name and has no involvement in the conflicted name process.[107] DNCL deems the conflict resolved in cases where the registrant indicated the preference of ‘do not want and do not object to another registering it’. The name would be released for registration on a first come, first served basis.[108] Where registrants came to an agreement, they would advise DNCL who would then advise the agreed registrant of the opportunity to register the name.[109]

If more than one registrant held the name at the third level and expressed interest in registering the .nz equivalent, then a “conflict” exists. For example, if one registrant held “anyname.co.nz”, and another held “anyname.org.nz”, and both registrants have expressed interest in registering “anyname.nz”, the domain name would be “conflicted” and unable to be registered until the registrants resolve the conflict amongst themselves.[110]

DNCL runs the conflicted domain names process for registrants who hold conflicted domain names to agree amongst themselves who (if anyone) is able to register the shorter second level .nz name.[111] It allows those registrants who hold a registration at the third level the first right of refusal to register the second level .nz equivalent.[112] If more than one registrant held the name at the third level and expressed interest in registering the .nz equivalent, then a “conflict” exists.

InternetNZ data shows that, as at August 2019, 2,239 .nz domain names remain “conflicted” and 5,066 third level domain names are claiming rights to the second level .nz equivalents.[113] This is not a significant proportion of the 700,000 odd domain names registered so it could be considered not a “significant” issue. However, it may be an issue for those who are unable to

[106] Clause 10.2 of the .nz Operations and Procedures Policy.
[107] Clause 10.3 of the .nz Operations and Procedures Policy.
[108] Clause 10.4 of the .nz Operations and Procedures Policy.
[109] Clause 10.6 of the .nz Operations and Procedures Policy.
[110] Clause 10.9 of the .nz Operations and Procedures Policy.
[111] Ibid.
[112] Clause 10 of the .nz Operations and Procedures Policy.
[113] There may be two or more claimants for each domain name.

resolve the conflict. Further, there is no specified end date in the policies to resolve .nz conflicted domain names.

If two third level domain names both have claims to the second level .nz domain, and are registered to the same individual or organisation, they are considered ‘self-conflicted’. As at August 2019, at least 318 .nz domain names are self-conflicted. The organisations or individual must resolve this self-conflict by lodging a preference through DNCL.[114]

Other ccTLDs have been through a similar process of opening up registration directly at the second level. These ccTLDs have used different methods to New Zealand in prioritising registrants’ rights to the domain name when a conflict arises:

- In 2012 the Japanese ccTLD, .jp gave priority to the holders of the Trademark *identical* to the proposed second level domain name[115]

- The Malaysia ccTLD, .my and Peruvian ccTLD, .pe gave priority to the domain name that had been registered the *longest*[116]

- China ccTLD .cn, and Philippines ccTLD .ph, gave priority to those domain names that held the *.com*.[ccTLD] domain name

- Canada, .ca and the United Kingdom, .uk have conflicted names processes most akin to .nz, where conflicts are resolved through *consent or bidding*. In addition, CIRA, has discontinued new registrations at the third level, so all new .ca domain names will be at the second level.[117]

auDA has announced intentions to begin allowing registrations at the second level and run a conflicted domain names process similar to the one for .nz.[118] Priority will be given to those who have registered before a cut-off date, and if multiple registrants have equal priority, there is a conflicted domain status until they resolve it; they must continue to pay an annual application fee and satisfy the eligibility and allocation criteria for a licence.

[114] DNCL, https://www.dnc.org.nz/conflicted-name-process/lodge-your-preference/
[115] Japanese Network Information Centre, https://www.nic.ad.jp/timeline/en/
[116] MYNIC, https://www.mynic.my/en/about-us-milestone.php
[117] Clause 3.5, ‘Conflicting Names’ https://cira.ca/policy/rules-and-procedures/general-registration-rules
[118] auDa, ‘AU Namespace Implementation’, see clause 1.9, https://www.auda.org.au/policies/index-of-published-policies/2019/au-namespace-implementation/

Questions for the Panel

We would like the panel to consider:

- What could the future of outstanding conflicted domain names look like to try and resolve the current situation of 2,000 plus remaining conflicted .nz domain names, and over 300+ self-conflicted domain names?

Unique Domain Authentication Identification (UDAI)

Under the .nz Operations and Procedures Policy, registrars and the registry may generate a new UDAI at any time.[119] A UDAI is a unique eight-digit code needed to transfer a .nz domain name from one Registrar to another.[120] Having the correct UDAI verifies that the registrant has the authority to make changes to the domain name.

Other TLDs have similar codes but may use the language of “Auth-code”, “authorisation code” or “info code”.[121] ICANN guidance for gTLDs states that registrars should provide the Auth-Code to the domain name holder in one of two ways:

- Allow the registrant to create its own Auth-Codes through a control panel, or
- Provide the Auth-Code within five calendar days of a request.[122]

The current .nz policies are consistent with ICANN’s gTLD guidance. They ensure that a UDAI generation function must exist, and enable the UDAI to be regenerated by the registry or registrar at any time. If registrars fail to provide the UDAI to a registrant, the DNCL may do so.[123]

Questions for the Panel

We ask the panel to consider:

- Are the current policies around UDAI generation still fit-for-purpose?

- Should the policies be technology neutral to provide the Registry more flexibility in providing authorization methods?

[119] Clause 14 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[120] DNCL, ‘Check your UDAI’, https://dnc.org.nz/udai

[121] ICANN, ‘About auth code’, https://www.icann.org/resources/pages/auth-2013-05-03-en

[122] Ibid.

[123] Clause 14 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

Billing registration length

We seek your views on the time period for when a registrant can be billed in advance of holding a licence.

Currently, the policies state that the registry is to bill for registration and renewal of domain names on a monthly billing period.[124] A domain name's billing period begins at the time it is registered or renewed and extended for the number of months indicated by the billing term. Registrars can initiate the renewal process at any time and advance renewals can be accepted as long as they are no longer than 120 months (10 years) from that date.[125] Registrars are billed for advance renewals.[126]

Market self-regulator (DNCL)

The responsibilities of DNCL, as the market self-regulator of the .nz domain, are set out in the .nz policies.[127]

The .nz Principles and Responsibilities Policy provides that, the obligations and responsibilities of DNCL are detailed in the .nz Registrar Authorisation Agreement.[128] The responsibilities set out in that document are the minimum standard of behaviour that DNCL expects to meet in its day-to-day relationships with the registry and the registrars and form part of the .nz policies. It also provides that DNCL will 'endeavour to ensure an open, competitive and fair market'.

The Registrar Authorisation Agreement sets out that DNCL will:

- Operate in a transparent, ethical manner, honouring principles of good faith and fairness
- Administer and enforce the .nz policies
- Authorise and, where appropriate, de-authorise registrars
- Recognise, promote, and protect the rights of registrants.

The policies currently require that, if DNCL is engaging with registrants direct, the registrar will be advised.

[124] Clause 13.1 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures and clause 5 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities
[125] Clause 13.6 of the .nz Operations and Procedures Policy and clause 5.1 of the .nz Principles and Responsibilities.
[126] Clause 13.6 of the .nz Operations and Procedures Policy.
[127] Clause 12 of the .nz Principles and Responsibilities Policy.
[128] Ibid.

Harmful and illegal activity

A pertinent question is whether the provisions of the .nz policies should be expanded to more proactively monitor online harm or illegal activity on the .nz domain name space.

InternetNZ data shows a growing concern about harmful and illegal content online. Colmar Brunton research found 92% of New Zealanders are concerned about young children being able to access inappropriate content, with online crime, identity theft and cyber bullying also ranking amongst New Zealanders biggest concerns.[129] Domain names can be used to cause such harms.

In addition to real harm caused to people, the .nz brand may be being leveraged for criminal activity, and the brand could be tarnished by this activity. The Domain Name Abuse forum hosted by InternetNZ and DNCL in November 2018 drew out stakeholder feedback seeking a more proactive approach.

New Zealanders may not be fully aware of the amount of online crime that now occurs using .nz domain names. A research survey found that .nz domain names are seen by New Zealanders as the most trustworthy and secure, compared to other TLDs.[130]

However, data mined by InternetNZ shows that one percent of a sample of 70,000 domain names analysed were possibly connected to fraudulent e-commerce sites. We do not currently have data on whether this is comparable to other ccTLDs.

Currently, the .nz policies determine that DNCL's overall position in relation to domain name abuse is to follow the rule of law and natural justice principles and leave these matters to the court.

The .nz policies require registrants to supply accurate information to the registrars and to use domain names only for legal purposes. The .nz Principles and Responsibilities Policy states the registrant, through their agreement with their registrar, has an obligation to "ensure the registrar's services, and the domain name, are not used for an unlawful purpose."[131]

[129] Colmar Brunton, 'Public Opinion Research', p. 36, https://internetnz.nz/sites/default/files/InternetNZ_public_opinion_research_results.pdf

[130] Ibid., p. 26-27, https://internetnz.nz/sites/default/files/InternetNZ_public_opinion_research_results.pdf

[131] Clause 9.1.5 of the .nz Principles and Responsibilities Policy

Additionally, the .nz policies provide a principle of 'no concern for use: the ccTLD manager is not concerned with the use of a domain name'.[132] Neither InternetNZ nor DNCL actively review how domain names are being used. DNCL has deferred to the courts as the appropriate determiner of online issues regarding how a domain name is used. The .nz Operations and Procedures Policy provides that DNCL does not have jurisdiction to consider complaints relating to:

- Illegal or malicious use of a domain name
- Objectionable or offensive website content
- Possible breaches of legislation.[133]

DNCL co-operates with New Zealand court orders regarding these abuses of domain names. From 1 March 2018 to 31 May 2019, DNCL was not served with any warrants or production orders.[134]

Sometimes members of the public or organisations name the Domain Name Commission Limited as a second respondent in legal proceedings. Typically, DNCL is named to assist with domain name takedowns and may have to disclose information to support the court. In April 2019, the DNCL was named as a second respondent about legal proceedings related to a Harmful Digital Communication Order. DNCL filed a Memorandum agreeing to abide by any order of the Court.

Acting in response to court orders means there is transparency and accountability for DNCL, and ensures that it is following New Zealand laws when it suspends a .nz domain name or makes information provision decisions. The trade off is DNCL often cannot respond quickly to the use of domain names causing immediate harm.

Expanding enforcement activity allowed by the .nz policy framework would require expanding DNCL's jurisdiction and necessitate public consultation.

The independent review by David Pickens found there are serious information deficiencies on the magnitude and nature of Internet related harm in New Zealand.[135] It stated, only with good information (relevant, timely, complete,

[132] Clause 2.1.5 of the .nz Framework Policy, https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf

[133] Clause 11.6 of the .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[134] Domain Name Commission Limited, 'Trust in the .nz domain name space', p. 5, https://dnc.org.nz/sites/default/files/2019-06/201819_transparency_report%20v0.2.pdf

[135] David Pickens, 'Final report: Domain Name Commission Limited (DNCL) Regulatory Review' p. 60 - 69, p. 64, https://dnc.org.nz/sites/default/files/2019-08/Pickens%20Report%20-%20Independent%20Regulatory%20Review%202019v0.1.pdf

accurate) will it be possible to effectively target real problems with the best tools available and can the effectiveness of strategies deployed be assessed.

The Pickens report notes that Internet harm is a global problem and there are a number of initiatives internationally to reduce opportunities for harm in the TLD space. The Security and Stability Advisory Committee within ICANN notes that attacks continue to be a significant problem for registries, registrants and their users, around the world. Risks identified included:

- phishing where malicious actors gain access to the Registry or a registrar through a legitimate looking email, resulting in compromise of the entire Registry/registrar, and

- "domain shadowing" where malicious actors use stolen or phished credentials to create multiple sub domains below existing legitimate domains.

The Security and Stability Advisory Committee noted the risks cannot be completely prevented and therefore recommends an incident response plan.[136]

The Pickens report makes a number of recommendations summarised below, including:

- facilitate the collection of key data across agencies so that the nature and magnitude of any issues relating to the .nz space might be better known, over time and against other TLDs where similar information is known, and so that the effectiveness of current and future enforcement efforts might be determined

- draw on international experience to date, in particular, the effectiveness of measures so far deployed and new measures being developed

- explore the importance of coordination and cooperation between countries and TLD operators for new measures to be effective - this could involve engagement with ICANN's Public Safety Working Group, for example

[136] David Pickens, 'Final report: Domain Name Commission Limited (DNCL) Regulatory Review', p. 62, https://dnc.org.nz/sites/default/files/2019-08/Pickens%20Report%20-%20Independent%20Regulatory%20Review%202019v0.1.pdf

- work with other agencies to develop an enforcement option that might better promote the public interest compared to the current strategy.

We ask the Panel to consider pages 60-69 of the David Pickens' report when thinking about how to overcome the issue of illegal activity and harm, and the role of the regulator (e.g. should it be expanded to more closely monitor and regulate against online harm and illegal activity) and other players in the New Zealand justice system. We would also like the Panel's views on how any changes may impact trust, security, openness, and privacy.

Emergency and exceptional circumstances

In the wake of the terrorist attack on Christchurch mosques on March 15 2019, an interim "emergency and exceptional circumstances" clause was inserted into the .nz Operations and Procedures Policy.

InternetNZ determined that DNCL needed a clear and certain provision in the .nz policies to ensure sites with terrorist material were able to be suspended or cancelled. A temporary approach was endorsed to deal with the urgent threat in the .nz domain name space while the nation was at the highest terrorist threat level.

An interim approach was endorsed when the temporary approach expired to ensure such material was not allowed in the .nz domain name space. This interim approach expires in October 2019 unless renewed (for a further six months) by InternetNZ.[137]

The interim clause in the .nz policies provides:

> *In emergency or exceptional circumstances (e.g. terrorist attack, cyber security or force majeure event) where the Domain Name Commissioner reasonably considers that use of the .nz domain name space is causing, or may cause, irreparable harm to any person or to the operation or reputation of the .nz domain space is causing, or may cause, irreparable harm to any person or to the operation or reputation of the .nz domain space, the Domain Name Commissioner may take action to mitigate or minimise that harm. Action taken under this clause shall be proportionate to the harm and is limited to the temporary transfer, suspension or locking of a domain name registration.*[138]

[137] The interim policy has now been extended for six months by the InternetNZ Council.

[138] Subject to clause 11.8, which enables the Commissioner to take action to minimise harm in an emergency or exceptional circumstance, https://internetnz.nz/nz-operations-and-procedures

DNCL has reported that one .nz domain name was suspended during the period where the National Threat Level was high through this interim measure because it had been hijacked.[139] The domain name was suspended for less than 24 hours and was reinstated once that material had been removed.

Infrastructure abuse and cyber attacks

We would like the Panel to consider how the .nz policies could enable us to act against infrastructure abuse using .nz domains.
Security threats and abuse issues on the Internet are often connected with domain name abuse. This type of abuse can emerge in two ways:

1. domain names being used in a deceptive way e.g. through phishing
2. use of domain name infrastructure for malware

Phishing domain names are used to deceive users into providing information to webpages that claim to be a trustworthy entity, like a bank.[140] It is often associated with financial fraud but can also be used to steal identities. Examples of phishing domains in .nz could include **ā**nz.co.nz, trade**we**.net.nz, phishpond.co.nz, or voda**ph**one.nz. These domains are often homographic, where letters, numbers or symbols that look similar to each other, such as the letter O and the number 0 are used to deceive an unknowing victim.

As the DNS is part of the Internet, malicious actors use the DNS infrastructure to host or facilitate intrusive software that is installed without consent – malware. These domain names are not typically seen by users, but play an important function in the command and control of malware.[141]

Domain name hijacking

Domain name hijacking is when an unauthorised person (typically from a criminal group) gains control over a domain registered to another individual or organization.

Hijacking can be accomplished through various practices and often results in domain name registrants losing control of their domains as traffic is redirected to a different site, the content of the original site is changed, or the outside agent switches the control of the name through the registrar.[142]

[139] DNCL, ‘Trust in the .nz domain name space’, https://dnc.org.nz/sites/default/files/2019-06/201819_transparency_report%20v0.2.pdf
[140] CERTNZ, https://www.cert.govt.nz/individuals/explore/phishing/?topic=phishing
[141] ICANN, ‘Malware’, https://www.icann.org/resources/pages/malware-2013-05-03-en
[142] ICANN, ‘Domain Name Hijacking’, https://icannwiki.org/Domain_Name_Hijacking

DNS Security Extensions (DNSSEC)

DNSSEC strengthens authentication in the DNS using digital signatures based on public key cryptography.

DNSSEC adds two important features to the DNS protocol:

- data origin authentication provides an assurance the DNS response came from the correct place

- data integrity protection prevents someone altering the content of a DNS response as it traverses the Internet.[143]

Currently, the .nz policies put the responsibility of managing DNSSEC with registrars and registrants.[144] DNSSEC can help protect the integrity of the DNS, and reduces the likelihood that registrants will suffer from a security incident. We seek your views on whether this provision is still appropriate.

We encourage the Panel to consider what the right settings are for the .nz domain name space to ward against infrastructure abuse and cyber attacks to promote legal, meaningful use of the Internet, and enables DNCL to proactively detect and take action against harmful uses of the DNS.

Sanctions

The current .nz Principles and Responsibilities Policy provides that sanctions can be imposed by DNCL to such conditions as DNCL considers fit.[145]Sanctions may be temporary or permanent and are at the sole discretion of DNCL.[146] DNCL must reasonably consider that any sanction is proportionate to the breach, having regard to all of the surrounding circumstances at the time it occurred, its consequences, and the purposes of the .nz policies adhering to principles of natural justice.[147]

Sanctions against any party to the Registry, Registrars and Registrants may include correction of any details in the Register and transfer or cancellation of domain names.[148] Sanctions against Registrars may include suspension of the Registrar's functions, entitlements or rights and registrar de-authorisation.[149]

[143] ICANN, 'DNSSEC: what is it and why is it important', https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

[144] Clause 12 of .nz Operations and Procedures Policy, https://internetnz.nz/nz-operations-and-procedures

[145] Clause 14.1 of the .nz Principles and Responsibilities Policy, https://internetnz.nz/nz-principles-and-responsibilities

[146] Clause 14.2 of the .nz Principles and Responsibilities Policy.

[147] Clause 14.3 of the .nz Principles and Responsibilities Policy.

[148] Clause 14.4 of the .nz Principles and Responsibilities Policy.

[149] Clauses 14.5.1 and 14.5.7 of the .nz Principles and Responsibilities Policy.

If register data is found to be incorrect then attempts will be made to correct it. If a registrant has obtained the domain name by fraud or deception then DNCL may cancel the domain name without warning.[150]

These sanctions may not be considered appropriate in today's context or sufficiently clear and certain. We seek your views.

Questions to Panel

We ask the Panel to consider:

- Are the provisions sufficiently clear on the regulator's (DNCL) role?
- Should the role of DNCL be expanded - for example, is there a role to more closely monitor content abuse? If so, for what reason, and what do you think is an appropriate approach?
- Should the .nz policies encourage or promote use of DNSSEC? If so, are the current provisions still appropriate and fit-for-purpose?
- Are the provisions on sanctions in the .nz policies sufficiently clear and appropriate in today's context?

Understanding the .nz policies

Principle-based regulation

The .nz policies are largely principle-based. The advantage of principle-based regulation is that it allows a degree of self-regulation without high transaction costs. The approach tends to work well in low risk sectors that require flexibility and innovation. The disadvantage of principle-based regulation is that is provides less clarity and certainty.

The principles we use to regulate the .nz space are set out in three documents:

- The Top Level Domain (TLD) Principles[151]
- The .nz Framework Policy (which sets out the principles governing the operation of the .nz TLD)[152]

[150] Clause 14.6.2 of the .nz Principles and Responsibilities Policy.
[151] InternetNZ, "TLD Principles", https://internetnz.nz/tld-principles
[152] InternetNZ, ".nz Framework Policy", https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf

- The .nz Principles and Responsibilities Policy (which sets out the principles under which the .nz domain name space is run and the roles and responsibilities of the parties involved).[153]

Procedures and operational matters are set out in another document.[154] The Operations and Procedures Policy covers a wide range of operational matters, such as the process for registering, managing and cancelling domain names, disputes and complaints, as well as the billing process.[155]

These are publicly available on the InternetNZ and DNCL websites.

Consideration of how the policies are set out and communicated

Standalone or separate policies

Currently, the .nz policies are contained in a number of stand-alone documents. Some argue this could be distracting or challenging for a participant to understand and use the policies, in particular how they relate to each other. On the other hand, stand-alone documents (when well curated) can allow each policy area to be clearly distinguished.

We ask the Panel to consider whether the arrangement of the .nz policies could be more user friendly. For example, should we follow the approach taken by government regulators which typically brings the elements of a regulatory regime together in one place? An example of this is the Telecommunications Act 2001 (and associated regulations) which contains provisions to regulate the supply of telecommunications services.[156] We are not asking for formatting or drafting suggestions, rather your views on the general approach.

Clear, plain English

Good practice in drafting regulation is to use clear, plain English. This practice allows a wide audience to understand potentially complex subject matter. This is particularly important when there are consequences if a person suffers penalties if they do not meet regulatory requirements.

[153] InternetNZ, ".nz Principles and Responsibilities Policy", https://internetnz.nz/nz-principles-and-responsibilities
[154] InternetNZ, ".nz Operations and Procedures Policy", https://internetnz.nz/nz-operations-and-procedures
[155] InternetNZ, ".nz Operations and Procedures Policy", clauses 7, 11, 13, 17, 18, 19.
[156] Telecommunications Act 2001, http://www.legislation.govt.nz/act/public/2001/0103/latest/DLM124961.html

We ask the Panel to consider whether the policies have the right balance between technical considerations and plain English. We are not seeking drafting suggestions, rather a general view on this question.

Accessibility

We would like to ensure that the domain name system and .nz policies are accessible to diverse groups of people across New Zealand in terms of age, ability, economic status, etc. We ask the Panel to consider this question.

Home of the .nz policies

The .nz policies are openly available on the websites of InternetNZ and DNCL. We ask the Panel to consider if there are other ways the .nz policies could be made available.

Glossary

More at DNC glossary here: https://www.dnc.org.nz/faqs

Acronyms

DNC - Domain Name Commissioner

DNCL - Domain Name Commission Limited

DNS - Domain Name System

DNSSEC - Domain Name System Security Extensions

IDN - Internationalised Domain Names

IRPO - Individual Registrant Privacy Option

TLD - Top Level Domain

ccTLD - country code Top Level Domain

gTLD - generic Top Level Domain

URL - Uniform Resource Locator, or more simply a web address

Domain name statuses (from DNC.org.nz)

Active - Means the domain name has been registered.

Pending release - Means the domain name has been cancelled and is in a 90 day pending release period. Only the current registrant can reinstate the name during this time.

Available - Means the domain name is available to be registered on a first-come first-served basis.

Prohibited - Means the domain name is prohibited under .nz policy from being registered.

Conflicted - Means the domain name is unable to be registered because equivalent names exist in at least two second levels. Before a conflicted name can be registered, it needs to be resolved.

Resolved - Means the domain name’s conflict status has been resolved. The registrant with resolved rights has two months from the date of resolution to register the name.

International bodies

ICANN - International Corporation for Assigned Names and Numbers.

ccNSO - The Country Code Names Supporting Organisation is a body within the ICANN structure created for and by ccTLD managers.

IETF - Internet Engineering Task Force is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite.

RFC - a Request for Comments is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature.