



January 2020

# Re-imagining the future of .nz

---

Issues report of the .nz Policy Advisory Panel

## Foreword

The past six months have been a challenging and truly rewarding ride as InternetNZ charged us ‘the Panel’ with conducting the most wide ranging review of policy in the organisation’s history.

Our panel of 10, each selected for their different but expert experience, has worked diligently and with great respect for each other’s perspectives, to identify the issues surrounding the current policies that shape and regulate the .nz domain name space.

To its credit, InternetNZ has encouraged the Panel to cast the net wide – seeking opinions of New Zealanders from all walks – from those who understand the internet intimately to people who, for whatever reason, have been excluded. InternetNZ’s [initial briefing](#) was drawn on as a launch pad for our thinking.

We have used formal research and less formal feedback to help frame this first report, identifying the issues we want to delve into more deeply or for which we require more feedback before we reach a view. We looked at what other regimes are doing to identify common issues and any best practice worth replicating. All feedback has been invaluable in guiding us to finalise this issues report.

This issues report considers the framework that regulates .nz and its interface with strategic objectives of internet openness, access, security and through important lenses of privacy, competition, e-commerce, human rights and Māori interests.

Emerging highlights from our thinking include the need to prioritise security whilst ensuring access and growth in the .nz domain name space and the potential to be a world leader in the recognition of indigenous rights.



None of this would have been possible without the outstanding contribution from the InternetNZ secretariat, particularly Kate Townsend, Kim Connolly-Stone and Nicola Brown who have been unstinting in their support of the panel and its various needs.

We are especially grateful to everyone who has contributed to our report, particularly those who shared personal experiences when participating in our online survey, focus groups and the Nethui session.

This is our first report. We look forward to consulting with people further on the issues we have outlined together with the solutions we will develop, before finalising our recommendations in the middle of this year on the future of .nz policies.

Finally I say thank you to InternetNZ for having the courage to let a bunch of outsiders have a thorough look under the hood.



**Sue Chetwin**

**Chair**

.nz Policy Advisory Panel

January 2020

## Executive Summary

From its research, analysis and engagement, the .nz Policy Advisory Panel ('the Panel') has identified the .nz policies contain a number of issues that need to be refined or solved. It intends to consult further to more fully understand stakeholder concerns, develop its own thinking and provide workable options and recommendations to these issues.

Specifically, in considering the guiding principles in the .nz policies, the Panel finds a number of priorities in the .nz domain name space in today's world are not evident or supported. Areas identified that require more explicit inclusion in the principles include security and trust, access, greater protection of individual private information, stronger growth in .nz as a digital asset and Māori interests.

Based on the work and engagement to date, the Panel has identified potential principles on which options will be developed and detailed consultation will need to be directed:

- A **trusted, secure** and safe .nz domain name space
- An **open and accessible** domain name space for all
- Development/Whanaketanga of the .nz domain name space as a digital asset to empower/enable New Zealanders to connect, create and **grow**
- Greater protection of **te reo and Māori** cultural interests.

The Panel found a range of perceived or actual barriers to accessing .nz. These barriers include a lack of knowledge and skills to register a domain name, cost, a perception you need to live in New Zealand, thinking other domain name extensions are more highly valued because of their greater global presence (e.g. .com), and cases of preferred domain names being unavailable.<sup>1</sup>

Linked to access, the main issue identified in the area of openness (aside from a general lack of understanding of the concept) that could pose an issue for security and growth is no geographical presence requirement exists for those who wish to register a .nz domain, unlike .au and .ca.

Opportunities exist to improve the security of the DNS infrastructure and to facilitate greater public confidence in the reliability of .nz domain

---

<sup>1</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study-focus groups', p. 9, 10, 29, 30,

<https://internetnz.nz/sites/default/files/2.2%20Final%20Rpt%20Focus%20Groups%20-%20Internet%20NZ%20-%20nz%20Policy%20Research%20-%20Nov%20>

names. Abuse of .nz domain name registration services, the malicious use of a .nz domain name and lack of oversight of reseller security practices were identified by the Panel as challenges to holding security and trust in .nz domain names.

The global trend to strengthen protection of an individual's data online through regulatory measures impacts New Zealand and the .nz space. The Panel identified the private information collected and held on a registrant could be considered inappropriate in today's world. The way it was publicly available may tip the individual's right to privacy and result in unintended consequences such as fake details being used or demotivating persons (particularly vulnerable people) to even register for a .nz.

The Panel identified issues where the .nz policies intersected with human rights. They include the rights to freedom of expression, to due process, and to freedom from discrimination. In many instances the current policies align with these principles. However, opportunities to show further respect for human rights exist.

The Panel is aware that responding appropriately to Māori interests is complex and would like to involve itself further with Māori communities as its thinking develops on solutions. Nevertheless, its initial assessment is the .nz policies in their current form do not provide the necessary protections for te reo and other important Māori interests.

The Panel found strong support to protect te reo in the .nz space from its stakeholder engagement but mixed feedback on whether there should be a strong connection to Te Tiriti o Waitangi (the Treaty of Waitangi) and .nz. The Panel wants to explore this issue further. It considers the .nz space could enable Māori to better connect and grow businesses in ways previously unavailable. New Zealand and .nz could take the lead on this issue globally.

Both survey respondents and UMR focus group participants highlighted opportunities for .nz to help businesses and e-commerce develop.<sup>2</sup> People thought .nz could be further leveraged to promote and grow opportunities for New Zealand businesses, and that .nz could be more creative and innovative.<sup>3</sup>

---

<sup>2</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 34-37, <https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results%20analysis%20and%20insights.pdf>

<sup>3</sup> UMR, 'Public perceptions of policy review for .nz: A qualitative study- focus groups', p. 41, <https://internetnz.nz/sites/default/files/2.2%20Final%20Rpt%20Focus%20Groups%20-%20Internet%20NZ%20-%20nz%20Policy%20Research%20-%20Nov%202019.pdf>

The survey research indicated registrants were relatively dis-empowered as end-line customers in the .nz market and that resellers lacked visibility and accountability. Also registrars could potentially be better incentivised to improve market competition and the registry's role may need to adapt.

# Contents

<b>Foreword</b>	2
<b>Executive Summary</b>	4
<b>Introduction</b>	8
<b>Background</b>	8
<b>Purpose of the review</b>	9
<b>The process</b>	10
<b>Guiding principles</b>	13
<b>Access</b>	21
<b>Openness and .nz</b>	26
<b>Security and Trust</b>	30
<b>Privacy</b>	36
<b>Human Rights</b>	42
<b>Te Tiriti and Māori interests</b>	46
<b>Growth: enhancing the .nz market place</b>	52
<b>Next steps</b>	59
<b>Appendix: the roles of .nz market participants</b>	60

## Introduction

The domain name system (DNS) is a vital component of the Internet - it allows people to easily access Internet resources.

New Zealand has a country code top level domain (ccTLD) assigned to it (.nz), to represent New Zealand on the Internet.

The Panel believes the policy and operating environment for .nz must be contemporary and that the contribution that .nz and the internet make to Aotearoa-New Zealand is maximised. It sees this as a critical element of the Internet stewardship in New Zealand.

The last comprehensive review of the .nz policies was in 2004. This review is being conducted by InternetNZ over 18 months. The .nz Advisory Panel is providing InternetNZ with independent advice over the first 12 months on the current policies that shape and regulate the local domain name space.

## Background

The .nz policy framework was established by InternetNZ and the Domain Name Commission Limited (DNCL) in the early 2000s. The policies have been reviewed and amended ad hoc since then.

In 2015, the framework was consolidated from 14 policies to the five policies currently in use. After an organisation restructure in 2018, InternetNZ assumed direct responsibility for the policies that regulate the local domain name space.

The .nz policy framework sets out the operation of the .nz domain name space. The policies were originally drafted in 2002 and have been revised from time to time:

- TLD principles<sup>4</sup>
- .nz Framework policy<sup>5</sup>
- .nz Policy development process<sup>6</sup>

---

<sup>4</sup> InternetNZ, 'TLD principles', <https://internetnz.nz/tld-principles>

<sup>5</sup> InternetNZ, '.nz Framework Policy', <https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf>

<sup>6</sup> InternetNZ, '.nz Policy Development Process', <https://internetnz.nz/nz-policy-development-process>

- .nz Principles and responsibilities<sup>7</sup>
- .nz Operations and procedures<sup>8</sup>
- .nz Dispute resolution service.<sup>9</sup>

The policies cover registration and management for .nz domain names, second level domain (2LD) structure, conduct of .nz registrars and resellers with sanctions for misuse or harm, handling of complaints and disputes and how the policy development process is to run.

## **Purpose of the review**

InternetNZ is comprehensively reviewing its .nz policies to identify how the Internet and .nz can continuously improve, and to ensure its principles and policies are fit-for-purpose.

The review allows the Internet and .nz community as well as the public to identify and raise issues that need a policy response now, or in future.

InternetNZ's .nz Policy Development Process (PDP) document allows for any party to identify possible policy requirements and notify these to InternetNZ or DNCL.<sup>10</sup> The PDP also provides that, once a policy topic has been identified, InternetNZ will define and scope it, including considering the rationale for the policy (or amendment of an existing policy).<sup>11</sup> InternetNZ has assigned the defining and scoping of policy changes to the Panel.

The Panel's remit is to provide policy, technical and operational input as well as seek wider stakeholder views and advice to help InternetNZ identify issues, develop options and recommendations, and lead community engagement.<sup>12</sup>

The Panel was asked to provide advice to InternetNZ through two reports:

- an Issues Report based on its findings by January 2020; and

---

<sup>7</sup> InternetNZ, 'Principles and Responsibilities', <https://internetnz.nz/nz-principles-and-responsibilities>

<sup>8</sup> InternetNZ, 'nz Operations and Procedures', <https://internetnz.nz/nz-operations-and-procedures>

<sup>9</sup> InternetNZ, 'nz Dispute Resolution Service', <https://internetnz.nz/dispute-resolution-service-policy>

<sup>10</sup> See clauses 4.1 the .nz Policy Development Process.

<sup>11</sup> See clause 4.2 of the .nz Policy Development Process.

<sup>12</sup> InternetNZ, 'nz Comprehensive policy review: Advisory panel terms of reference', <https://internetnz.nz/sites/default/files/DotNZ%20review%20panel%20ToR.pdf>

- a Recommendations report by July 2020.

InternetNZ is keen for the updated policies and principles to be robust and reflect the wider needs and expectations of the .nz Internet community and New Zealand society.

The review will consider the .nz policy framework that comprises the six policy documents listed above under “background”.

Notably, the InternetNZ Council is responsible for setting the overall long-term strategic direction for managing the .nz domain name space.<sup>13</sup>

## The process

The Chair of the .nz Advisory Panel, Sue Chetwin, was appointed in April 2019. Sue brings a wealth of governance experience from her position as Chief Executive Officer of ConsumerNZ, director of the Banking Ombudsman Scheme, member of the Online Media Standards Authority as well as the Electricity Authority’s Retail Advisory Group.

A well-rounded group of nine Panellists with a diverse mix of skills and knowledge were appointed in June 2019 to help champion this work and bring experience but also fresh, new perspectives. The Panellists are:

- Nita Wirepa
- Alma Hong
- Charlie Gavey
- Ty Kahu
- Mark Boddington
- Matt Brown
- Tim Johnson
- Mark Thomas
- Robert Rolls.

The Panel held its first meeting on 31 July which focused on establishing an operating model to deliver the two required reports.

During August and September, the Panel was provided presentations and an [initial briefing](#) from InternetNZ on key background information to assist its understanding of the domain name space. These presentations were on the:

- registry

---

<sup>13</sup> See clause 4.4 of the .nz Policy Development Process.

- technical research function
- regulator (DNCL)
- commercial function
- security function, and
- strategic pillars (openness and access).

From September to November 2019, Panellists undertook to identify the issues in the .nz domain name space. The Panel decided to frame its analysis around InternetNZ’s strategic objectives (access, openness, security) and to see the work through particular lenses (privacy, human rights, Te Tiriti and interests of Maori, and market growth).

In tandem, the Panel engaged New Zealanders to understand their views on the issues. This helped supplement the lack of available data. The Panel relied on three inputs and noted a fourth from industry:

- a session at NetHui on 3 October (‘Re-imagining the future of .nz’)<sup>14</sup>
- public submissions on a survey (276 responses received)<sup>15</sup>
- further research with “hard to reach” stakeholders through focus groups<sup>16</sup> and telephone interviews<sup>17</sup> run by research agency, UMR
- noted a report from the Registrars Advisory Group (RAG) in response to InternetNZ’s initial briefing on the .nz policies.

In October to December 2019, the Panel analysed the issues and drafted this report for the InternetNZ Council. The Panel has woven stakeholder feedback on the issues related to the .nz policies as well as its own research and thinking to shape its Issues Report.

To help with the analysis, the Panel received international insights from two inputs prepared by the Secretariat:

- a briefing on how the international domain name space is governed and important international organisations

---

<sup>14</sup> NetHui 2019, ‘The future of .nz - discussion session’,  
<https://livestream.com/accounts/4547920/events/8835617/videos/197289272>

<sup>15</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’,  
<https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results%20analysis%20and%20insights.pdf>

<sup>16</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’,  
<https://internetnz.nz/sites/default/files/2.2%20Final%20Rpt%20Focus%20Groups%20-%20Internet%20NZ%20-%20nz%20Policy%20Research%20-%20Nov%20>

<sup>17</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth telephone interviews’, p. 8 & 14,  
<https://internetnz.nz/sites/default/files/2.3%20Final%20Rpt-%20Internet%20NZ%20-%20nz%20Policy%20Research%20-%20Depth%20interviews%20-%20Nov%202019.pdf>

- meetings with three similar jurisdictions (Canada, Australia and the United Kingdom) about how their domain name space is managed.

The Panel provided its report to the InternetNZ Council on 14 February 2020.

A key part of the Panel's second phase of work which begins from February is exploring solutions to the issues that have been identified. It will make its final recommendations report to the Internet NZ Council by July 2020.

## Guiding principles

### Background

The Panel recognises the importance of reviewing the current principles to identify how InternetNZ can continuously improve and ensure its principles and policies that regulate the .nz domain name space remain fit-for-purpose in a dynamic industry.

Principles form an important role in a policy framework setting out what the policies seek to achieve and guide the implementation and interpretation of the .nz policies and procedures. Clear principles can provide direction and a unifying dimension to a shared organisational purpose and make it easier for stakeholders to understand the policy priorities. This is particularly true when the policy environment involves issues of public interest and where the specific policy issues can be technical.

The revised .nz principles will serve as a guide or “rule of thumb” in regulating the .nz domain name space. InternetNZ has two key policy documents that refer to principles. The principles within these documents are set out below:

The current principles from the .nz Framework Policy include:<sup>18</sup>

- **Rule of law** - the laws of NZ apply and the lawful instructions of the courts and authorities made 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

---

<sup>18</sup> InternetNZ, ‘.nz Framework Policy’,  
<https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf>

consistent with this policy, the .nz policies and associated agreements and contracts.

Internet NZ also has a set of principles that it uses to think about the operation of all TLDs:<sup>19</sup>

1. Domain name markets should be **competitive**
2. **Choice for registrants** should be maintained and expanded
3. Domain registrations should be **first come, first served**
4. Parties to domain registrations should be on a **level playing field**
5. Registrant data should be made **public**
6. Registry / registrar operations within a TLD should be **split**
7. Top Level Domain policy should be determined by open **multi-stakeholder** processes.

Principles are also included in a third policy document, .nz Principles and Responsibilities.<sup>20</sup> These principles relate to the market environment, registrations, financials, moderated second level domain names, and register data.

InternetNZ entered into a Memorandum of Understanding (MoU) for the Management of the .nz ccTLD with the Ministry of Business, Innovation and Employment in 2016.<sup>21</sup> Clause 9 of the MoU references the principles that guide InternetNZ's work in the domain name space. The Panel will consult government and wider stakeholders on proposed changes to the policies.

## Identified Issues

The Panel has examined the principles in the three documents and considered stakeholder feedback as well as its own views in reflecting on the principles. It has considered whether the principles are relevant in today's world, if they will endure over the next 10 years and if there are any gaps. The key omissions in the principles are set out below. The Panel also provides its observations about the format and construction of the principles.

---

<sup>19</sup> InternetNZ, 'nz TLD principles', <https://internetnz.nz/tld-principles>

<sup>20</sup> InternetNZ, 'nz Principles and responsibilities', <https://internetnz.nz/nz-principles-and-responsibilities>

<sup>21</sup> The MoU was updated in June 2018.

## **Current principles don't always reflect today's world and stakeholder priorities**

The Panel considers that the principles should better reflect important and relevant contemporary issues as well as align more strongly with stakeholder priorities.

### **Access**

The Panel notes the absence of a reference to access in the principles which would support breaking down barriers for people to register in the .nz domain name space.<sup>22</sup>

The research findings are set out in more detail under the “access” section below. However, generally, UMR research participants noted barriers to access .nz that included a lack of knowledge and skills to register a domain name, cost, a perception you need to live in New Zealand, a perception that other domain name extensions are more global, and a preferred domain name was vetoed or unavailable.<sup>23</sup>

Although the online survey results found only 5% of respondents consider the people who want or need to access .nz do have access to it, a large number of respondents (over 44%) ‘did not know’.<sup>24</sup>

The Panel considers the explicit omission of access in the guiding principles does not help reduce barriers to .nz and it needs further feedback on this aspect before it makes a recommendation.

### **Openness**

The Panel believes the current principles do not articulate a vision of “openness” for .nz.<sup>25</sup> In fact, the principles could sometimes limit openness. For example, the principle of “registrant rights come first” currently prioritises one group (registrants) and does not capture the importance of other groups or consider all New Zealanders.<sup>26</sup>

---

<sup>22</sup> Notably, the Panel has not yet observed “access” built into other ccTLD’s principles.

<sup>23</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 9, 10, 29, 30.

<sup>24</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 20: Notably, 38% responded in the affirmative that people who want or need to access .nz do have access.

<sup>25</sup> The Panel defines “openness” as the extent to which .nz supports people to participate online, creating new uses of .nz and innovate. It used this definition for its online .nz survey in September 2019.

<sup>26</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 9.

The Panel would like to further consult on this area to determine the importance of explicitly including openness in the principles.

## **Security**

The principles do not make an explicit reference to promoting security or trust in the .nz domain name space instead preferring a hands-off approach.

The Panel considers security is an increasingly significant area for the .nz domain name space.

UMR focus group participants also wanted greater transparency and visibility of security operations in the management of .nz as a priority.<sup>27</sup> The majority in the UMR telephone interviews considered security as one of the most important areas in which InternetNZ should focus (followed closely by access and privacy).<sup>28</sup>

Many (42%) online survey respondents submitted they felt .nz is not secure, somewhat secure or has average levels of security.<sup>29</sup> Only 36% of respondents thought security was good or high. Respondents felt a more visible approach on security would increase confidence in the security of .nz.<sup>30</sup>

The Panel thinks explicit reference to security in the principles is needed to signpost the importance of security.

---

<sup>27</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study-focus groups', p. 13, 42-43 & 45.

<sup>28</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study-in depth telephone interviews', p. 8 & 14,  
<https://internetnz.nz/sites/default/files/2.3%20Final%20Rpt-%20Internet%20NZ%20-%20nz%20Policy%20Research%20-%20Depth%20interviews%20-%20Nov%202019.pdf>

<sup>29</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 2, 9-13.

<sup>30</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 10.

## Privacy

The Panel considers the current principles may not sufficiently provide support for individual privacy needs.

Today, people are increasingly concerned at the collection, storage and release of their own personal information.<sup>31</sup> In the UMR telephone interviews, participants felt privacy of information was one of the top policy focus areas for InternetNZ.<sup>32</sup> The TLD principle, “Registrant data should be made public”, does not align with New Zealand privacy laws.

The Panel wishes to consult further for fuller feedback on privacy and .nz before it determines if and how to include it in the principles.

## Human Rights

Human rights are not explicitly referred to in the principles. The lack of visibility and guidance from this omission may not reflect stakeholders’ expectations. The majority (80%) of the online survey respondents considered human rights to be important.<sup>33</sup>

However, the UMR focus group participants struggled to find a direct link between .nz and human rights.<sup>34</sup> Additionally, the Panel found other similar ccTLDs do not see a strong need to include human rights in their principles and defer to local law where human rights are protected.<sup>35</sup>

We consider the current “rule of law” principle captures the need to adhere to human rights obligations prescribed in applicable law (as well as other legal obligations more broadly). However, the Panel would like to consult on whether an explicit reference to human rights is necessary and a reference to illegal or objectionable content is also necessary.

The Panel would like further stakeholder feedback on this issue to help make recommendations on it.

---

<sup>31</sup> InternetNZ Secretariat, ‘.nz Survey: summary and analysis’, p. 25.

<sup>32</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth telephone interviews’, p. 14.

<sup>33</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 32.

<sup>34</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 35.

<sup>35</sup> The Panel observed this in meetings with the UK, Canada and Australia. Notably, GAC Working Groups on Human Rights and International Law (HRIL WG): within ICANN, there is the GAC Working Group on Human Rights and International Law that is looking at how the coordination of the domain name system is managed in a way that respects human rights, <https://gac.icann.org/working-group/gac-working-groups-on-human-rights-and-international-law-hril-wg>

## **Growth and the .nz marketplace**

More than 50% of respondents to the Panel's online survey felt .nz policies were critical to support New Zealand business.<sup>36</sup> Respondents to the online survey as well as UMR participants said more awareness and activity were needed to promote e-commerce.<sup>37</sup>

The UMR focus group participants thought .nz could be leveraged to promote and grow opportunities for New Zealand businesses and other enterprises.<sup>38</sup>

The Panel notes the existing principles cover competition.<sup>39</sup> However, it believes there are opportunities to better support .nz business and e-commerce growth, as well as broader Māori, social and other enterprise .nz development.

The Panel also looked at how the existing .nz market operates, particularly concerning the role of registrants, registrars, the registry and resellers. The Nethui session and UMR research broadly confirmed to the Panel that registrants are relatively dis-empowered as end-line customers in the .nz market.<sup>40</sup> Resellers are not visible and lack accountability in the market. Also registrars could potentially be better incentivised to improve market competition and the registry's role may need to adapt to address this.

The Panel believes further consultation in this area would be valuable to devise appropriate solutions in this overall area which the Panel has called "growth".

## **Te Tiriti and Māori Interests**

The principles for .nz do not contain any reference to Te Tiriti o Waitangi (Te Tiriti) or any acknowledgement to protect Māori interests.

---

<sup>36</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 35.

<sup>37</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 34; UMR, 'Public perceptions of policy review for .nz: a qualitative study-focus groups', p. 37-38, 41-44; UMR, 'Public perceptions of policy review for .nz: a qualitative study-in depth telephone interviews', p. 14.

<sup>38</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 13, 42-44.

<sup>39</sup> InternetNZ, 'nz Framework Policy', <https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf>; InternetNZ, 'TLD principles', <https://internetnz.nz/tld-principles>

<sup>40</sup> NetHui 2019, 'The future of .nz - discussion session', <https://livestream.com/accounts/4547920/events/8835617/videos/197289272>; UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups'.

The Panel recognises Te Tiriti creates a partnership between Māori and the Crown unique to New Zealand but it notes InternetNZ and most of its partner agencies are non Crown entities.

The Panel notes many survey respondents considered Te Tiriti should not be considered as part of .nz (43 of 161 responses) and the focus group research also felt the management of .nz should not reflect Te Tiriti.<sup>41</sup>

However, general support for protection around the use of te reo Māori in the .nz space was shown and a smaller selection of the UMR research (the telephone interviews) found Te Tiriti should be acknowledged.<sup>42</sup>

The mixed feedback from this initial engagement highlights further consultation is required before the Panel devises options for how to address Māori interests in the principles.

### **Inadequate guidance and inaccessible format and language**

The Panel has identified the following issues with the principles related to inadequate guidance and inaccessible format and language:

- **certain principles are operational** rather than providing direction on a shared organisational purpose or guide to regulating the overall .nz space. A few principles explain what is expected in registering domain names, such as “First come first served - any domain name can be registered if available for registration on a first come, first served basis”.<sup>43</sup> The Panel considers such principles would sit better in the operational parts of the policies (not the guiding principles)
- the .nz policies or surrounding documents **provide no guidance when tension** arises between the principles. The Panel considers this likely creates confusion for users and may not lead to optimal outcomes. The Panel found it hard to understand the circumstances, for example, when ‘registrant rights come first’ in one area how this then impacts on the first come first served principle. No guidance exists on how principles interact with each other, how to resolve tensions, or how to reach an optimal balance between them

---

<sup>41</sup> A minority of the online survey respondents felt Te Tiriti should be included (10 out of 161 responses): InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 29.

<sup>42</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- qualitative telephone interviews, p. 6, 12. InternetNZ Secretariat, ‘.nz survey: p. 30.

<sup>43</sup> InternetNZ, ‘.nz Framework Policy’,

<https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf>

- the **multiple documents are not accessible** with principles spread across three distinct documents from two organisations (InternetNZ and DNCL). This confuses users about how the principles are used to regulate the .nz domain name space, and when. No common landing page or index exists to easily show all policies in one place. A recent Google search for “.nz policies” led to a link to the DNCL not InternetNZ webpage as the first result.<sup>44</sup> That link contains links to four of the six policies and no reference to the .nz framework principles or TLD principles policies. In addition, a search for ‘.nz policies’ on the InternetNZ homepage does not return a comprehensive list of the policies (it also omits the two policy documents containing the principles)
- the **language of the principles is not accessible**: some principles are drafted in an operational or technical manner using industry jargon. Many registrants and potential registrants will not know many of the terms, such as “no concern for use”, “first come first served” or “ccTLD”. A reader unfamiliar with these terms could unwittingly be non-compliant
- the current **“rule of law” principle could be less prominent**. This principle sets out that the laws of New Zealand apply and the lawful instructions of the courts and authorities will be complied with. The Panel considers this should not be a principle rather it is implicit in how the .nz domain name space operates as also exemplified by how other similar ccTLDs treat it.

## Low levels of awareness

Although not a policy issue, a point to note is the need for InternetNZ to increase awareness and education of the benefits of .nz. This feedback was strong in the online survey and in the UMR research.<sup>45</sup> The survey found less than 10% of respondents were aware of the .nz policies.<sup>46</sup> The Panel does not have a full understanding of why there is such low levels of awareness but notes it is consistent with other ccTLDs like Canada, UK and Australia. Participants submitted that InternetNZ as the manager of .nz has the responsibility to improve in these areas.<sup>47</sup>

---

<sup>44</sup> A Google search in December 2019 found this link:

<https://www.dnc.org.nz/the-commission/policies>

<sup>45</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 13, 42 & 45, and InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 6.

<sup>46</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 7-8.

<sup>47</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 7, 8.

## Access

### Definition of access

The Panel considers “access” to mean that people who want a .nz domain name have the know-how and skills to set up one and use it, and can afford to do so.<sup>48</sup>

### Background

The Panel has found varied feedback on barriers to access the .nz domain name space.

Informed by the research and stakeholder engagement, the Panel has identified issues and challenges to access to the .nz space including a lack of understanding, knowledge and skills as well as potential barriers with the .nz policies being only in one language and domain names are predominantly in English.

This area has strong links to the growth section below in this report.

### Identified issues

#### Lack of understanding, knowledge and skills

The Panel found from its engagement that people lack the understanding, knowledge and skills to know about the .nz domain name space.<sup>49</sup> Many people confused it with telecommunications or the Internet more broadly.<sup>50</sup>

This lack of understanding is a concern because, as a community resource, it is a crucial part of people confidently sharing and engaging in many of the various benefits of the space.

Nearly a third of respondents to the online survey (38%) thought the people who want or need access to .nz domain names in fact have access.

<sup>51</sup> Nearly half of respondents (44%) did not know if they had access issues

---

<sup>48</sup> This definition was used in the Panel’s online survey on .nz to the wider public.

<sup>49</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 7-8, 13, 18, 19, 23, 43.

<sup>50</sup> For instance, in response to the access question, online survey respondents considered the cost of maintaining a web presence including email hosting and website development too high.

<sup>51</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 21.

with .nz. For the open ended question, about a third of respondents also cited a lack of knowledge or awareness about how to use domain names as a barrier to access .nz.<sup>52</sup>

The UMR research also showed stakeholders have a general lack of understanding or know-how in accessing the .nz domain name space.<sup>53</sup> Many participants in the UMR focus groups viewed the Internet as an important part of modern life but had never sought to purchase a domain name. Barriers to access .nz domain names expressed by participants included a lack of knowledge and skills to register a domain name (raised by seniors), cost, a perception you need to live in New Zealand, and not knowing who are the trusted registrars.<sup>54</sup>

In particular, the “business” group in the UMR focus groups considered barriers to access include:

- they only have limited skills to develop a website
- the cost may be too high
- gTLDs are better for scaling their business
- a preferred domain name was vetoed or unavailable.<sup>55</sup>

The “senior” group in the UMR focus groups particularly felt they lacked knowledge and skills. The “youth” group were more confident in their ability to access .nz but placed less value on it because it is not perceived as global (like .com).

The Panel’s initial view therefore is that many New Zealanders feel they lack the skills and knowledge or ability to access the .nz domain name space. However it would like to hear more from stakeholders during consultation.

### **Lack of accessibility from English-only policies**

The .nz policies are drafted only in English. New Zealand is now a multicultural society, far more so than when the policies were formulated. Digitally excluded communities exist.<sup>56</sup> The language or style in which the

---

<sup>52</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 22.

<sup>53</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 7, 9, 18.

<sup>54</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 9, 10, 29, 30.

<sup>55</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 12.

<sup>56</sup> Motu Economic and Public Policy Research, ‘Digital inclusion and wellbeing in New Zealand’, October 2019

policies are drafted, and that of the registrar's terms and conditions, may not provide access to people who speak other primary languages.

The Panel considers the .nz policies need to be in plain English. It notes Australia's auDA has recently revisited its policies and is undertaking to ensure all documents will be drafted in plain English.<sup>57</sup>

Despite stakeholders not raising this as an issue in the engagement phase, the Panel considers the current policies in English-only may prevent access to the .nz domain name space. It therefore wishes to consult on whether any access issues would be overcome if the policies were translated into other languages, or simply in a more plain English style.

### **Inhibiting access to .nz by restricted characters in domain names**

The Panel considers the way that only English and macrons can be used to register a .nz domain name may restrict access to those people who speak other primary languages and who want to register a domain name. Macrons are able to be used. However the Panel would like to test during consultation whether the policies should go further in allowing an expanded range (for example, Arabic or Vietnamese character sets) to enhance access to .nz domain names.

Australia is looking at introducing Internationalised Domain Names (IDNs) to support and reflect an ethnically diverse and multicultural country.<sup>58</sup> In addition, the United Kingdom in 2012 created gTLDs under ICANN's related program for Welsh people. Under this program there are implementation areas where the cultural aspects have been made distinct (e.g. reserved names lists and accented character sets).<sup>59</sup>

### **Costs to register or renew a .nz domain name**

Many submitters were unsure of the cost of a .nz in both the online survey and the UMR focus groups. However they considered the cost needs to be more widely published or known and it needs to be "affordable", otherwise

---

<https://motu.nz/our-work/wellbeing-and-macroeconomics/well-being-and-sustainability-measures/digital-inclusion-and-wellbeing-in-new-zealand/>

<sup>57</sup> Panel meeting with auDA on 28 November 2019.

<sup>58</sup> Afilias, 'IDNs and the development of a multilingual DNS for .au, 20 August 2019, <https://afilias.com.au/newsroom/blog-posts/idns-and-development-multilingual-dns-au>

<sup>59</sup> Nominet, 'Registrar resources', <https://registrars.nominet.uk/gtlds/gtld-registrar-systems/internationalised-domain-names-idns/>

it is a barrier to access.<sup>60</sup> This issue connects also to the areas of “growth” discussed in a section below.

If there is uncertainty around the value of .nz domain names this could lead to a loss of confidence and relative value.<sup>61</sup> Interestingly, online survey respondents thought gTLDs (like .com) are cheaper.<sup>62</sup>

When informed of the annual cost to register a wholesale .nz domain name (NZ\$1.25 per month or \$15 per year), UMR focus group participants thought this cost is not a barrier to access.<sup>63</sup> Participants generally viewed a price of under \$100 a year to register as affordable for individuals.<sup>64</sup> Some support was given by the senior and youth groups for a sliding scale where individuals and small businesses pay less while large businesses pay more.<sup>65</sup> The business group interviewed were less keen on a sliding scale model. Businesses viewed it as fairer to have one base rate that applies to everyone.<sup>66</sup> Notably, when prompted, the community groups thought cost was a barrier (including internet connection cost).<sup>67</sup>

Wholesale costs and pricing structures vary across ccTLDs. Notably, the retail price will vary depending on the registrar.<sup>68</sup> The Panel observed:

- the UK’s Nominet (.uk) sees the immense benefits of domain names to the digital economy and strives to make access affordable and easy. The wholesale cost is £3.90 (NZD\$7.70) per year<sup>69</sup>

---

<sup>60</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 10, 29, 30 and UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth interviews’, p. 11; InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 18.

<sup>61</sup> If there is uncertainty in the .nz cost, confidence could drop and the relative value with it, particularly compared to other domain name extensions.

<sup>62</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 18, 19, 22.

<sup>63</sup> Notably, registrars may add cost to this wholesale price; UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 41.

<sup>64</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 10 & 30, and UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth interviews’, p. 11.

<sup>65</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 10.

<sup>66</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 30.

<sup>67</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth interviews’, p. 15.

<sup>68</sup> The retail price varies by registrar, see Nominet, <https://www.nominet.uk/change-to-uk-domain-wholesale-prices/>

<sup>69</sup> Nominet’s .uk price used to be £80. It then dropped to £20 and subsequently £5 in the early 2000s.

- the wholesale price for .au domain names starts from A\$8.67 (NZD\$9.03) per year (and does not vary). Registrars have discretion to set the retail price<sup>70</sup>
- the wholesale price for a .ca domain name is CA\$9.50 (NZD\$10.97)<sup>71</sup>
- .com by comparison is priced at USD\$7.85 per year.<sup>72</sup>

Based on stakeholder feedback, the Panel concludes while the current price to register a domain name is below \$100 per year for individuals (and around \$20-30) then it is likely not an issue.<sup>73</sup> However, if the retail cost to register a .nz is over \$100 per year for non-business registrants this will likely create a barrier to access in future. The .nz policies will need to be updated accordingly if a change to the pricing structure is made. Greater public awareness through publishing detailed costs could be beneficial.

## Digital exclusion

While addressing digital inclusion is outside the scope of this review, the Panel would like to note the policy framework needs to acknowledge the role of supporting access for digitally excluded communities.

---

<sup>70</sup> auDA, <https://www.auda.org.au/industry-information/registrars/registrars-accreditation/>

<sup>71</sup> CIRA, [Registrar Fees List](#)

<sup>72</sup> Businesswire, ICANN and Verisign Announce Proposed Amendment .com Registry Agreement',

<https://www.businesswire.com/news/home/20200103005209/en/ICANN-Verisign-Announce-Proposed-Amendment-.COM-Registry>

<sup>73</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study-focus groups', p. 30.

# Openness and .nz

## Definition of openness

InternetNZ published a “Defining Openness” paper in October 2019.<sup>74</sup>

The Panel considers “openness” for the context of the .nz review to mean: .nz supports people to participate online, creating new uses of .nz and the ability to innovate.<sup>75</sup>

## Background

Globally, Internet openness is recognised as contributing to economic growth and social wellbeing.<sup>76</sup> A domain name is the address connecting people to the Internet where they can share and disseminate information and knowledge. Internet openness is also relevant to the domain name system in a number of ways because it enables technical features such as a consistent address space and a uniform convention for domain names.<sup>77</sup> However, in reality, it depends how the domain name is used and the parameters around it.

The Panel found in its research and engagement stakeholders have a low understanding of “Internet Openness” related to domain names. There are opportunities to work better with communities in this area. The majority of respondents (65%) submitted to the online survey question ‘is .nz as open as it needs to be?’ that they do not know.<sup>78</sup> Some respondents (28%) considered it is as open as it needs to be; most of these respondents (88%) were people who sell domain names.<sup>79</sup>

The UMR focus group work also found participants had difficulty understanding what openness meant in relation to .nz. Participants suggested InternetNZ should tailor its messaging on openness to better

---

<sup>74</sup> InternetNZ, “Internet Openness”, [https://internetnz.nz/sites/default/files/IntNZ\\_Internet\\_Openness\\_Final\\_Digital.pdf](https://internetnz.nz/sites/default/files/IntNZ_Internet_Openness_Final_Digital.pdf)

<sup>75</sup> The Panel used this definition for its online .nz survey in September 2019.

<sup>76</sup> See for example OECD, “Economic and Social Benefits of Internet Openness” (OECD Digital Economy Papers No. 257, 2016), <https://doi.org/10.1787/5j1wqf2r97g5-en>

<sup>77</sup> OECD, “Economic and Social Benefits of Internet Openness”, p. 9, (OECD Digital Economy Papers No. 257, 2016), <https://doi.org/10.1787/5j1wqf2r97g5-en>

<sup>78</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 17, 18.

<sup>79</sup> Ibid., p. 15; UMR, ‘Public perceptions of policy review for .nz: a qualitative study- in depth telephone interviews’, p. 10.

communicate with various New Zealand communities and raise its profile to educate the public.<sup>80</sup>

Informed by the research and stakeholder engagement, the Panel has identified policy issues (below) related to Internet openness and the .nz space.

## Identified issues

### **No clear definition of openness**

The Panel considers it is an issue that there is no unequivocal definition for Internet Openness and its connection with .nz in the policies. Without a common understanding, people find it challenging to effectively contribute to the topic. This is an issue on which the Panel would like to further consult.

### **No geographical limits on registrants**

Currently, there are no geographical limits to acquire a .nz domain name or a requirement for registrants to have a “New Zealand” presence. This issue is pertinent for the area of openness of .nz but it also connects to the areas of access and security set out in this report.

During the Panel’s engagement, people often assumed a .nz domain name required a “New Zealand presence”. When informed there was no current geographical limit, some respondents in the UMR research were surprised foreigners could register a .nz. They considered a geographical requirement would contribute to the value and security of the .nz domain space.<sup>81</sup>

Many respondents to the online survey and to the UMR work expressed low confidence in the security status of .nz and felt a local presence requirement would improve confidence in the security of .nz if registered by New Zealanders.<sup>82</sup> Business respondents felt New Zealand businesses

---

<sup>80</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study-in depth telephone interviews’, p. 10, and UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 9.

<sup>81</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- in depth telephone interviews’, p. 8, 15, UMR, ‘Public perceptions of policy review for .nz: a qualitative study-focus groups’, p. 13.

<sup>82</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 11-12, and UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 8, 9, 12.

wanting to export may generally prefer a .com TLD unless offering a unique Kiwi product.<sup>83</sup>

NetHui participants also pointed out a geographical presence requirement would contribute to the value and security of the .nz domain name space through reduced harm and increased accountability of domain registrants.<sup>84</sup>

The Panel received feedback from the Registrar Advisory Group (RAG) that adopting a geographic presence requirement after .nz had been unrestricted for many years would be impractical.<sup>85</sup>

The Panel observed both open and restrictive practices in other ccTLDs:

- the UK's Nominet, like InternetNZ, has open registrations for .uk. Nominet staff told the Panel that, given the diaspora of United Kingdom citizens, it was considered inappropriate to apply a geographical restriction to the .uk ccTLD
- by contrast, Canada's CIRA (.ca) aims to "keep .ca Canadian".<sup>86</sup> CIRA staff said they considered this geographical presence requirement contributed to reducing and managing harms in .ca
- the Australian ccTLD (.au) requires a nexus to Australia.

The Panel therefore considers the openness or level of restriction on who can register a .nz domain to be a key issue for further consideration and consultation to ensure the .nz policies and public expectations align. Decisions around openness are likely to also have implications on the areas of security and the market.

### **Minimum age requirement for .nz registrants**

The minimum age requirement of 18 years old for .nz registrants was noted by InternetNZ as a potential issue in considering who has access to a .nz domain name.

Today, young Internet users are able to create and publish content across a wide variety of platforms. The minimum age requirement for common social media platforms such as Snapchat, Youtube, Facebook and Twitter is

---

<sup>83</sup> UMR, Public perceptions of policy review for .nz: a qualitative study-focus groups', p. 37.

<sup>84</sup> NetHui 2019, 'The future of .nz - discussion session', <https://livestream.com/accounts/4547920/events/8835617/videos/197289272>

<sup>85</sup> Registrar Advisory Group, 'Response to the Initial briefing for .nz Panel from InternetNZ' p 6, (unpublished), November 2019.

<sup>86</sup> CIRA, "Keeping .CA Canadian", December 2019, <https://cira.ca/ca-domains/register-your-ca/keeping-ca-canadian>

13.<sup>87</sup> The .nz policies require a person to be at least 18 years old, which indicates the .nz policies may not reflect expectations around how children engage online today.

However, as this issue was not raised during public consultation, the Panel will not take it forward. It is not considered a major issue. In keeping with the expected structure of the outputs resulting from this review, the Panel believes registrant age is likely to be a purely operational concern that falls into the procedures of the registry and does not need to be addressed in the policies.

---

<sup>87</sup> Netsafe, “Social Media Advice for Parents: What are the age restrictions?”, 21 October 2019, accessed 16 December 2019, <https://www.netsafe.org.nz/social-media-parents/>

# Security and Trust

## Definition of security and trust

“Security and trust” refers to two loosely related concepts. One is information security practices that protect the .nz space from threats to its stability and security of the domain name space. The other is efforts to reduce the harmful use of .nz domains. This section is concerned with the latter - combatting “domain name abuse”.

## Background

Security and trust are vital to the success of the New Zealand .nz domain name space. They underpin .nz’s popularity in terms of website visits and the domain name customer base.

Security and trust are diminished by illegal or unlawful conduct or content in the .nz space.<sup>88</sup> The malicious activities of unknown threat actors such as domain hijackers, as well as legitimate registrants who conduct phishing and run fake online stores, dilute public confidence in the .nz space.

The Panel is examining whether policies that regulate the .nz domain name space promote a secure and trusted infrastructure, and facilitate public confidence in the reliability of .nz domain names.

The .nz Panel sought information about security and trust from .nz market participants and the wider public. A number of security related concerns were expressed by stakeholders.<sup>89</sup> In general, feedback indicated any policy reform should consider and, where possible, facilitate enhanced security and trust in the .nz space.

---

<sup>88</sup> Results from the .nz survey showed visible security failures negatively affect confidence in .nz, see: InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 11.

<sup>89</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 11 - 15.

## Identified issues

### Domain name registration abuse

Domain name registration services are a target for those who intend to abuse New Zealand's DNS. Domain name registration abuse is often the first step in a calculated campaign to make malicious or illegal use of a .nz domain name. Malicious registrants will often use fake or invalid details to avoid legal consequences.

Ensuring accurate registration details are captured by the registry can mitigate threats to security and trust.<sup>90</sup>

Currently, the Registry presumes registration information supplied by the Registrar is accurate. It does not validate details at the point of registration.

The DNCL, as market regulator, has authority to sanction registrants whose registration details are found to be invalid or fraudulent.<sup>91</sup> The DNCL's registration detail validation process involves contacting registrants and requesting they validate their contact details. Failure to respond or to validate their contact details results in the cancellation of the domain name.

While validation of details is useful, it is reactive. Some harm is necessary in the .nz space to initiate the process. This reactive process may mean a higher number of cases of abuse are happening but are undetected, and potential abusers are undeterred.

### Grace periods and domain tasting

The .nz policies provide for a grace period<sup>92</sup> which enables cancellation of a new domain name registration or renewal within five days. Grace periods are widely used by ccTLD managers because they enable mistakes to be corrected and permit registrants to rectify failed payments without losing their domain name service.

Grace periods may be exploited for purposes that diminish security and trust. For example, grace periods enable "domain tasting", the practice of registering a domain name with the intention of cancelling within the grace

---

<sup>90</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 12.

<sup>91</sup> Clause 7.7 of the .nz Operations and Procedures, <https://internetnz.nz/nz-operations-and-procedures>

<sup>92</sup> Clause 7.11 of the .nz Operations and Procedures.

period to avoid costs. This practice is commonly used by those mining traffic.<sup>93</sup> However, grace periods may also support more malicious activities such as phishing. Whether this is a problem in the .nz space is unknown.

The Panel has been advised by the RAG that the majority of registrants are unaware of the registration and renewal grace period, and how it benefits them.<sup>94</sup>

## **Misleading and deceptive domain names**

The Panel received a small amount of feedback about malicious activities that deceive visitors to a website with a .nz domain name into thinking they are interacting with a website with a legitimate domain. One example was typosquatting which can facilitate phishing and other domain name abuse.

Some respondents expressed concern about typosquatting, the practice of registering a domain name that was misleading or confusingly similar to a popular domain name.<sup>95</sup>

The potential for fraud and phishing risk with macronised vowels was also considered by the Panel. The current policy permits separate registration of macronised and non-macronised versions of the same domain name.

InternetNZ advised the Panel of overseas ccTLD managers' policies supporting IDN adoption that were relevant to the issue of security and trust.<sup>96</sup> CIRA in Canada permits French accented characters to be registered. Once a registrant has registered a domain name, variations of the domain name with these accented characters are then bundled and reserved for the registrant, preventing registration by anyone else. This is known as an administrative bundle.

The lack of feedback from the engagement process indicates the public is unaware of this issue or does not consider it to be a significant threat to security and trust in the .nz space.

---

<sup>93</sup> InternetNZ Secretariat, 'An Initial briefing for .nz Panel from InternetNZ (Part Two)' p. 5, [https://internetnz.nz/sites/default/files/Briefing\\_for\\_the\\_.nz\\_panel\\_part\\_2.pdf](https://internetnz.nz/sites/default/files/Briefing_for_the_.nz_panel_part_2.pdf)

<sup>94</sup> Registrar Advisory Group, 'Response to [the] Initial briefing for .nz Panel from InternetNZ', (unpublished), November 2019, p. 6.

<sup>95</sup> McAfee, 'What is Typosquatting?', <https://www.mcafee.com/blogs/consumer/what-is-typosquatting/>

<sup>96</sup> InternetNZ Secretariat, 'An Initial briefing for .nz Panel from InternetNZ (Part Two)' p. 19-20, [https://internetnz.nz/sites/default/files/Briefing\\_for\\_the\\_.nz\\_panel\\_part\\_2.pdf](https://internetnz.nz/sites/default/files/Briefing_for_the_.nz_panel_part_2.pdf)

Nevertheless the Panel is interested in hearing views on the adoption of an administrative bundle policy equivalent to CIRA's and the feasibility of implementing a 'prohibition on misspellings policy', and what this could resemble.

## **Domain and website content abuse**

The Panel was presented with sufficient evidence to suggest illegal or unlawful conduct and content in the .nz domain space is a live issue, despite the exact nature and magnitude of domain and website content abuse being unknown.

Feedback indicated some malicious activities were more prevalent and caused more concern than others. In particular, phishing and fake online stores were identified as being significant threats to security and trust.<sup>97</sup> Less concern was expressed about the sale of illicit goods and services, and the dissemination of other forms of illegal or objectionable website content. The one exception being content related to acts of hatred and violence such as the terrorist attacks on Christchurch mosques on March 15 2019.<sup>98</sup>

InternetNZ advised the Panel an interim emergency and exceptional circumstances clause was inserted into the .nz Operations and Procedures Policy following the Christchurch terror attacks.<sup>99</sup> This approach gave the DNCL the ability to temporarily transfer, suspend, or lock a domain name registration in circumstances where the use of the .nz domain name space is or may cause irreparable harm to any person or the operations or reputation of the .nz domain space.

Otherwise the malicious use of a domain name is not subject to regulation. The current principle "no concern for use"<sup>100</sup> means DNCL may only sanction a registrant for malicious use of a .nz domain when and as directed by the New Zealand courts in most cases.

During the engagement phase, the Panel asked stakeholders about their views on early intervention to minimise harm caused by illegal or

---

<sup>97</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 11 - 15; UMR, 'Public perceptions of policy review for .nz: a qualitative study - focus groups', p. 9.

<sup>98</sup> UMR, 'Public perceptions of policy review for .nz: A qualitative study - focus groups', p. 11 & 35, and UMR, 'Public perceptions of policy review for .nz: a qualitative study - in depth telephone interviews', p. 33.

<sup>99</sup> Clause 11.8 of the .nz Operations and Procedures, <https://internetnz.nz/nz-operations-and-procedures>

<sup>100</sup> .nz Framework Policy, <https://internetnz.nz/sites/default/files/SUB-NZF-dotnz-framework-policy.pdf>

objectionable content. A small number of respondents (2) thought InternetNZ should hold a position against hate speech and abuse on .nz. Conversely, a small number (2) thought .nz should remain a neutral service and not make content decisions.<sup>101</sup>

The Panel would like to consult further on the role of the DNCL in reducing Internet related harm and whether it should expand its regulatory role with respect to malicious use of a .nz domain. The Panel is conscious this may be a divisive issue. The Panel would also like to hear about ways DNCL could assist other organisations in reducing Internet related harm.

## **Registrar security**

The Panel has identified registrar security to be a policy issue as well as an operational concern for individual registrars. Compromised security at the registrar level has implications for the security of the registry and registrant, and accordingly can affect people's trust in the entire .nz domain name space.<sup>102</sup>

Currently, the registry has no explicit mandate to oversee the security practices of registrars.

The Panel considers the criteria to become a registrar may be inadequate to ensure .nz is secure. The process of becoming an authorised registrar focuses on technical capability and does not permit monitoring and evaluation of security practices. Moreover registrars are not incentivised or mandated to invest in adequate security standards or to adopt new technologies to safeguard .nz.

The introduction of new security products by InternetNZ may mitigate the risk of registrar security being compromised. An example is the proposed registry lock service.<sup>103</sup> With some registry locks, a registration cannot be modified unless the registrant gives the registry approval. The Panel is mindful that the introduction of new security technologies may necessitate

---

<sup>101</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 5.

<sup>102</sup> The United Kingdom's National Cyber Security Centre recently reported the most common form of DNS hijacking happened at the registrar level by malicious actors gaining unauthorised access to a registrant's account, see: Advisory: Ongoing DNS hijacking and advice on how to mitigate at p. 3, (Report, National Cyber Security Centre 12 June 2019), <https://www.ncsc.gov.uk/files/Advisory-DNS-hijacking.pdf>

<sup>103</sup> InternetNZ, Minutes of the .nz Policy Committee (2 April 2019), <https://internetnz.nz/sites/default/files/2019-04-05%20Minutes%20.nz%20Policy%20Committee%20-%20Final.pdf>

reconsideration of the roles and responsibilities of .nz market players within the current suite of policies.

### **Technology specific approach**

The Panel was advised by UMR that interviewees expected InternetNZ to be constantly improving security in the .nz space.<sup>104</sup>

The current suite of policies are technology specific. They refer to Osecurity products such as DNSSEC.<sup>105</sup>

During the engagement, a technical respondent commented on the limited uptake of DNSSEC internationally and questioned its future utility.<sup>106</sup> The Panel's own research indicates only three authorised .nz registrars meet the criteria to be deemed 'DNSSEC friendly' and six accept delegation signer (DS) records.<sup>107</sup>

The Panel is also aware of the .nz registry considering introducing other security products, for example the aforementioned registry lock service.

These developments suggest the current technology specific (as opposed to technology neutral) approach has implications for the longevity and the enduring quality of the policies. The Panel will work through possible options to overcome this issue in the coming months.

---

<sup>104</sup> UMR, 'Public perceptions of policy review for .nz: A qualitative study - Focus groups', p. 9.

<sup>105</sup> Clause 11.8 of the .nz Operations and Procedures, <https://internetnz.nz/nz-operations-and-procedures>

<sup>106</sup> InternetNZ Secretariat, '.nz survey: summary and analysis', p. 13.

<sup>107</sup> Domain Name Commission Limited (DNCL), 'Authorised Registrars', 26 November 2019, <https://dnc.org.nz/registrars>

# Privacy

## Definition of privacy

The Panel is looking at privacy through the lens of personal information that is collected, stored and disclosed.

## Background

When a .nz domain name is registered, contact details are collected as part of the process. Each .nz domain name has associated contact data, including registrant contact, admin contact and a technical contact.

According to the Registrant Core Terms and Conditions,<sup>108</sup> details to be collected for each of the contact sets include: name, email, address, country and phone number.

These details are referred to as the “WHOIS details”. The WHOIS system allows people to access the contact details of a specific domain.<sup>109</sup> The WHOIS terminology has been replaced by the DNC as the ‘Query Service’. The term WHOIS details is still widely used in the sector.

In 2017, the Individual Registrant Privacy Option<sup>110</sup> (“IRPO”) was introduced following a comprehensive review involving five public consultations and calls from many in the Internet community for greater privacy protection.<sup>111</sup>

The IRPO is an optional feature for individuals who are “not in significant trade”. A registrant can choose to use the IRPO and withhold the telephone number and contact address information provided to the .nz Query Service. IRPO is opt-in, meaning it is not selected by default.

The Domain Name Commission (DNCL) introduced a free provisional address masking option where individual registrants who hold .nz domain names can ask that their contact address be masked from public display in the WHOIS (domain search tool). This option came about due to apparent

---

<sup>108</sup> DNCL, ‘.NZ Registrant Agreement Core Terms and Conditions v2.1’, July 2018, [https://dnc.org.nz/sites/default/files/2019-09/registrant\\_agreement\\_core\\_terms\\_and\\_conditions\\_2.1.pdf](https://dnc.org.nz/sites/default/files/2019-09/registrant_agreement_core_terms_and_conditions_2.1.pdf)

<sup>109</sup> DNCL, ‘Domain Name Registration Data Query’, <https://www.dnc.org.nz/whois>

<sup>110</sup> DNCL, ‘Individual Registry Privacy Option’, <https://dnc.org.nz/irpo>

<sup>111</sup> DNCL, ‘WHOIS Review’, <https://dnc.org.nz/whois-review>

concern from some individual registrants about the public display of their contact address for privacy and personal safety reasons.<sup>112</sup>

Registrant data can be disclosed through a number of possible avenues:

- a public 'Query Service' to look up a specific domain<sup>113</sup>
- Query results which include either:
  - full contact details for registrants who have not opted for IRPO or who are ineligible for IRPO or;
  - non-withheld data for registrants who have opted for IRPO
- general written request, which could result in disclosure of 'Withheld Data'<sup>114</sup>
- court order or requirement of law, which could result in disclosure of 'Withheld Data'<sup>115</sup>
- entities under an MOU with automatic or streamlined access to 'Withheld Data'.<sup>116</sup> Only CERT NZ and the Digital Safety division of the Department of Internal Affairs (DIA) are listed as having this type of access (although the DIA does not appear to be listed on the MOU web page).

In addition to registrant data in the context of the above, aggregated data could be sensitive depending on the granularity. For example, registrations per city or suburb could lead to inference of registrants in places with low population.<sup>117</sup>

The Panel found during the Nethui session that a number of people confused online security with registrant privacy matters, demonstrating a lack of public understanding of privacy issues (in the context of a .nz domain) and general security or cyber safety issues.<sup>118</sup> Participants in the UMR focus groups also had limited experience with domain names and assumed privacy measures were applied to all information collected.<sup>119</sup>

---

<sup>112</sup> DNCL, 'Provisional address masking option', 2016, <https://www.dnc.org.nz/pamo>

<sup>113</sup> Clause 21.1 of the Operations and procedures policy.

<sup>114</sup> Clause 22.2 of the Operations and procedures policy.

<sup>115</sup> Clause 22.3 of the Operations and procedures policy.

<sup>116</sup> Clause 22.25-22.4 of the Operations and procedures policy.

<sup>117</sup> Clause 23.0 of the Operations and procedures policy.

<sup>118</sup> NetHui 2019, 'The future of .nz - discussion session', <https://livestream.com/accounts/4547920/events/8835617/videos/197289272>

<sup>119</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 31.

## Identified issues

The Panel has identified the below issues related to privacy and .nz based on the engagement process, existing views and international practice.

### Level of registrant data collected and stored

During the Panel's session at NetHui 2019, an issue was raised about the level of registrant information collected and stored and their lack of awareness that it is held and disclosed in some cases. Attendees questioned the purpose and need to capture such detailed information about registrants (e.g. physical address) and if less data (e.g. only name and email address) would be satisfactory without exposing registrants to undue privacy concerns.<sup>120</sup>

The UMR focus group participants were mostly against publishing full contact information because it was seen as unnecessary for the public to have access to it. One participant recounted unwanted contact from a person who had accessed their contact details.<sup>121</sup> However, another participant advocated for details to track a person that held the domain name they wanted to purchase.

The Panel heard at the Nethui session, and it was also raised in the online survey, that some registrants provided false contact information to protect themselves in response to the default of registrant information being publicly available (in violation of the registrant terms and conditions).<sup>122</sup> An inherent tension became clear between openness and accuracy of information and the need for greater protection of a registrant's individual data. The principles, enacted through policy, must decide which of these is of greater importance.

Further concerns were raised at the Nethui session over capturing overly detailed information from vulnerable groups.<sup>123</sup> These vulnerable persons may need to prevent certain information (e.g. physical address) from being publicly accessible. The Panel also considers this may link to access in that

---

<sup>120</sup> NetHui 2019, 'The future of .nz - discussion session'.

<sup>121</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 10.

<sup>122</sup> NetHui 2019, 'The future of .nz - discussion session'; results from the .nz survey indicated some registrants provide false information to protect personal privacy: InternetNZ Secretariat, '.nz survey: summary and analysis', p. 3; Registrant Core Terms 2.2: make sure all information you give us is accurate and complete, keep us informed of changes to any information you give us, and that you have the authority to enter into this agreement.

<sup>123</sup> NetHui 2019, 'The future of .nz - discussion session'.

it could likely demotivate a person to register a .nz when they find out about the level of their personal information captured, held or potentially disclosed.

Whilst the Panel has not yet formed a view on the appropriate level of registrant information to capture, it is clear the current policies and procedures place far greater weight on openness of registrant information than for those participants in the market providing services (e.g. resellers). Any changes to registrant information captured needs to consider this balance. The Panel views this to be a major issue but it wishes to consult further to assess and determine a fit-for-purpose solution.

### **Registrant data is made public by default**

The extent of registrant information made publicly available and the opt-out (rather than opt-in) nature of this information was raised as a concern during the .nz Panel's NetHui session.<sup>124</sup> Attendees had low awareness of which information was made public and also low awareness of the process for opting out of this information sharing. It was noted the opt-out process is not available to resellers.

Some respondents to the online survey including those who hold .nz domain names were concerned their details were freely available online through WHOIS (at least 13 of the 71 respondents to the open privacy question specifically raised this as an issue).<sup>125</sup>

In the UMR focus groups and telephone interviews, participants had difficulty connecting how there may be privacy issues in relation to .nz. Most participants could not see the necessity to collect full details and for them to be available to the public.<sup>126</sup> A few participants raised specific concerns over this issue and one participant had been negatively impacted from having their contact details publicly available, accessed by another and endured ongoing (unwanted) contact.<sup>127</sup>

---

<sup>124</sup> NetHui 2019, 'The future of .nz - discussion session'.

<sup>125</sup> InternetNZ Secretariat, 'nz survey: summary and analysis', p. 25, [https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results\\_%20analysis%20and%20insights.pdf](https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results_%20analysis%20and%20insights.pdf)

<sup>126</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 31; UMR, 'Public perceptions of policy review for .nz: a qualitative study- in depth interviews', p. 11.

<sup>127</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 31.

The RAG did not appear to highlight any issues related to privacy in its report.<sup>128</sup> It seemed to generally support the IRPO framework, but did stress the importance of privacy not being an option for “those engaged in significant trade”.

The Canadians have a similar framework to the .nz IRPO. Specifically, there is a distinction between individuals and organisations. Individuals receive privacy protection by default, whereas organisations do not. CIRA does provide for organisations to apply for privacy protection for special cases/requests.<sup>129</sup>

The .uk WHOIS does not publish a registrant’s details unless the registrant has given consent. Nominet provides registration data to third parties with legitimate reasons, such as enforcement of legal rights or use of its Dispute Resolution Service.<sup>130</sup> To obtain non-public data, a Data Release Request must be submitted with the submitter’s details (which will be disclosed to the data subject), and the reasons they have the right to access non-public data.

auDA also protects the privacy of registrants on the API and web service WHOIS through the use of roles, such as CEO, Director, domainadmin, etc. This is to minimise the exposure of individuals’ data and removes the need to update those contacts when a staff member moves on.

The .nz policies need to consider not only which information is captured about registrants, but whether registrants are given sufficient visibility and control of how their data is being used and shared. When considering operational implications for the management of personal data, international and domestic changes to privacy legislation (e.g. GDPR) will help shape both legal obligations and registrant expectations around how data is managed.

One of the existing .nz policies’ guiding principles, “registrant data should be public”, is in direct conflict with the IRPO framework implemented in 2017 that permits registrant data to be made private (not public).<sup>131</sup> While the IRPO makes it mandatory for registrars to offer the option for registrants to opt out of their information being made public, the requirement for registrants to opt in to privacy significantly reduces the

---

<sup>128</sup> Registrar Advisory Group, ‘Response to the Initial briefing for .nz Panel from InternetNZ’ (unpublished), November 2019.

<sup>129</sup> CIRA, ‘CIRA privacy policy’, <https://cira.ca/policy/corporate/cira-privacy-policy>

<sup>130</sup> Nominet, ‘Releasing your personal data to third parties’, <https://www.nominet.uk/privacy-notice/releasing-your-personal-data-to-third-parties/>

<sup>131</sup> DNCL, ‘Individual Registrant Privacy Option’, <https://dnc.org.nz/irpo>

effectiveness of the IRPO. The policies need to be driven by a clear direction around individual privacy concerns for registrant data.

### **Implementation of the IRPO and access to registrant information when required**

The 'Procedure for Disclosure of Withheld Data' (OP Section 22) may not be accessible/easy enough to satisfy people concerned about keeping registrant contact details available for disclosure in certain circumstances. However, concern still exists by the online survey respondents that they might be unable to access such data under legitimate circumstances. Similarly, the Panel questions whether the current implementation of IRPO provides enough transparency to the registrant, that contact details can still be disclosed to certain agencies under an MOU.

# Human Rights

## Definition of human rights

The Panel considers “human rights” to mean internationally recognised human rights that come from widely adopted human rights declarations, conventions and other instruments.

## Background

The Panel is investigating the relationship between .nz policies and human rights. The focus is to identify whether the current policy may lead to adverse human rights impacts.

InternetNZ is legally obliged to respect human rights that are enshrined in applicable national laws. In addition, InternetNZ and by extension the .nz policies should respect international human rights norms in accordance with internationally accepted frameworks such as the United Nations Guiding Principles on Business and Human Rights.<sup>132</sup>

The majority of respondents who completed the online survey thought human rights were important (44.5%) or extremely important (35%) in the context of the .nz policy review.<sup>133</sup>

The Panel has identified issues where the .nz policies intersect with human rights. They include the rights to freedom of expression, to due process, and not to be subjected to discrimination. These are discussed below. Other human rights are addressed elsewhere in this report, for example the right to privacy. To avoid repetition these issues will not be discussed further here.

## Identified Issues

### Domain names as a form of self-expression

A domain name may be a form of self-expression as well as an identification string. Individual registrants may use a domain name to express something about themselves to other people. In this sense domain name registration can be thought of as an expressive act.

---

<sup>132</sup> United Nations, ‘Guiding principles on business and human rights’, <https://www.business-humanrights.org/en/un-guiding-principles>

<sup>133</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 31-32, [https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results\\_%20analysis%20and%20insights.pdf](https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results_%20analysis%20and%20insights.pdf)

Current domain name registration policy imposes minimal restrictions on what words may be registered. This policy safeguards the expression “function” of domain names by granting registrants a high level of freedom and autonomy. Any word may be registered as a domain name so long as its use is not prohibited under legislation,<sup>134</sup> and it conforms to the relevant Internet standards as well as technical .nz policy requirements.<sup>135</sup>

Imposing few restrictions on domain name availability shows respect for freedom of expression but it also may negatively impact indigenous rights where eligibility requirements and the adoption of reserved lists could be considered to be more appropriate policy responses. For further discussion see the section titled, “Protecting te reo Māori in .nz domain names” in the Te Tiriti and Māori interests part of this report. Consideration of this issue may also have implications for the .nz principles of first come, first served and no concern for use.

## **IDN adoption**

The Panel recognises that people should be free to express themselves in their own language and considers the adoption of IDNs to be relevant to this right. New Zealand is an increasingly multicultural society and our largest city, Auckland, is especially ethnically and linguistically diverse.<sup>136</sup> With this in mind, and looking to auDA’s recent decision to adopt IDNs,<sup>137</sup> the Panel would like to consult further on the development of a multilingual domain name space for .nz.

## **Website content in the .nz domain space**

The principle “no concern for use”<sup>138</sup> has, until recently, insulated the .nz market participants from making value judgements about the suitability of content and accordingly has ensured the .nz policies respect people’s right to freedom of expression in this regard.

The introduction of the emergency clause<sup>139</sup> complicates matters. For example, it is not possible to reconcile “no concern for use” with an

---

<sup>134</sup> See for example: Flags, Emblems, and Names Protection Act 1981

<sup>135</sup> Clause 5.6 of the .nz Operations and Procedures policy.

<sup>136</sup> StatsNZ “2018 Census totals by topic – national highlights”, September 2019, <https://www.stats.govt.nz/information-releases/2018-census-totals-by-topic-national-highlights>

<sup>137</sup> auDA, “auDA Licensing Rules”, June 2019, <https://www.auda.org.au/index.php/policies/index-of-published-policies/2019/auda-licensing-rules/>

<sup>138</sup> Clause 2.1.5 of the .nz Framework Policy.

<sup>139</sup> Clause 11.8 of the .nz Operations and Procedures policy.

arbitrary power to suspend a domain name for content related activity. However, the Panel recognises freedom of expression is not absolute and is of the view that an emergency clause is a thoughtful and appropriate inclusion to the policies. Further, the Panel has considered the text of the clause and concluded the powers are suitable in the circumstances anticipated by the clause.

Whether the DNCL's powers to regulate content should be expanded to combat hate speech and other forms of objectionable content was a question posed to stakeholders during the engagement phase. The findings are discussed further in the Security and Trust part of this report - an area the Panel wishes to seek further information during public consultation.

### **Trusted notifiers and the right to due process**

The .nz Framework principles make specific reference to the “rule of law”. This principle makes explicit that an individual's right to due process is respected by the .nz policies in circumstances involving allegations of registrant criminality.

The DNCL's use of trusted notifiers to identify unlawful content may have implications for respecting due process. CERT NZ and the Department of Internal Affairs (DIA) were used by DNCL as trusted notifiers immediately following the terrorist attacks on Christchurch mosques on 15 March 2019. CERT NZ notifications are also used to inform the DNCL's response to domain name registration abuse. However, the .nz policies do not make explicit mention of the use of “trusted notifiers” in this context.

The Panel is also mindful that the need to regulate illegal and unlawful content in the .nz space may require more use of “trusted notifiers” such as enforcement agencies like the New Zealand Police. The Panel recognises the benefits of this approach in terms of expediency and harm reduction but is also conscious of the potential for these relationships to adversely impact registrants' right to due process where enforcement agencies' expertise, combined with a desire for a rapid response to minimise harm, serves as the basis for suspending a domain name.

### **Cultural rights and freedom from discrimination**

To avoid discrimination and to promote equal rights, it may be necessary to provide for particular groups in the .nz policies. Favouring groups known to have been discriminated against is recognised as a legitimate basis for unequal treatment. The Panel is conscious of potential opportunities to show greater respect for human rights in the .nz policies, especially with respect to indigenous rights and awareness of multiculturalism. The Panel

notes the current dispute resolution service enforces western intellectual property rights but does not provide an effective remedy for Māori traditional knowledge disputes. Further discussion on this and other relevant issues can be found in the Te Tiriti and Māori interests part of this report.

# Te Tiriti and Māori interests

## Background

The Panel is exploring whether InternetNZ policies sufficiently provide for the protection of indigenous rights in the management of the .nz domain name space. Māori are the indigenous peoples of Aotearoa-New Zealand.

New Zealand's founding document is considered to be Te Tiriti o Waitangi. It was signed between the British Crown and approximately 540 Māori rangatira (chiefs) in 1840.<sup>140</sup> The New Zealand Human Rights Commission views Te Tiriti as an important “living document” that establishes a relationship “akin to partnership” between the Crown and rangatira conferring a set of rights and obligations on each Te Tiriti partner.<sup>141</sup>

A 2018 New Zealand government report prepared for the United Nations report on the state of human rights in this country specifically highlights issues related to Maori and protecting te reo, education, skills and employment issues.<sup>142</sup>

Numerous opinions and conjecture exist about the interpretation and application of Te Tiriti in a modern context. Since the signing many organisations have included in their strategic documents and policies particular wording that sets out how they will acknowledge and give effect to Te Tiriti.

Almost all government departments and crown entities have references to Te Tiriti in their policies and plans that look to ensure they meet their obligations. The New Zealand Transport Agency, for example, has a Māori strategy called Te Ara Kotahi. It states:

*‘The Transport Agency recognises and respects Te Tiriti o Waitangi and will work with Māori to build strong, meaningful and enduring relationships to achieve mutually beneficial outcomes. Te Ara Kotahi (our Māori Strategy) provides strategic*

---

<sup>140</sup> New Zealand History, ‘The Treaty in brief’, p. 1, <https://nzhistory.govt.nz/politics/treaty/the-treaty-in-brief>

<sup>141</sup> Human Rights Commission. ‘Human rights and the Treaty of Waitangi’, [https://www.hrc.co.nz/files/2414/2388/0497/HRNZ\\_10\\_Human\\_Rights\\_and\\_the\\_Treaty\\_of\\_Waitangi.pdf](https://www.hrc.co.nz/files/2414/2388/0497/HRNZ_10_Human_Rights_and_the_Treaty_of_Waitangi.pdf)

<sup>142</sup> MFAT, Third National UPR Report, 2018, <https://www.mfat.govt.nz/assets/Uploads/New-Zealand-Third-National-UPR-Report-as-submitted-to-UN.pdf>

*direction to the Transport Agency on how we work with and respond to Māori as the Crown's Treaty partner, and what this means for how we do business.*<sup>143</sup>

The Panel notes that InternetNZ partner organisations such as Netsafe, Tohatoha Aotearoa Commons, TUANZ, the 20/20 Trust and also the Chief Censors' Office do not appear to refer to Te Tiriti or Māori issues in their goals or values. These are typically not-for-profit or independent entities without the more direct Crown mandate of a government department.

While InternetNZ is not part of the Crown, the Panel believes there is an opportunity for .nz to provide a leadership role with the development of appropriate and relevant indigenous Internet policies.

## Issue identification

The Panel has considered Te Tiriti and Māori interests in the context of the .nz policies through its own investigations and weighing up feedback from stakeholders.<sup>144</sup>

Despite mixed stakeholder feedback, the Panel believes the way in which Te Tiriti should impact .nz policies needs further careful reflection. Te Tiriti is acknowledged and applied in modern contexts and this .nz policy review is an important opportunity to address key interests that are not being met in the management of the .nz domain name space for Māori and to ensure inclusive policies that empower Māori are evident in the management of .nz where possible.

The Panel has identified potential issues related to Māori interests, including considering Te Tiriti, protecting te reo Māori in domain names, protecting the use of Māori.nz and iwi.nz domain names and the lack of culturally appropriate provisions in the .nz policies.

## Considering Te Tiriti and Māori interests

The .nz policies do not contain explicit provisions linked to Te Tiriti and Māori interests and there is no explicit mention of Māori interests in the principles. Many New Zealand organisations or government agencies (e.g.

---

<sup>143</sup> NZTA, 'Te Ara Kotahi - NZTA Maori strategy', <https://www.nzta.govt.nz/assets/About-us/docs/te-ara-kotahi-our-maori-strategy-june-2019.pdf>

<sup>144</sup> The Panel has engaged with a small proportion of the Māori community at this point and the content expressed within this document should not be considered a final representation of Māori views.

DIA) that have identified Māori as key partners and/or stakeholders have very established partnership or engagement frameworks.<sup>145</sup>

Feedback suggests people have mixed understandings of Te Tiriti and Māori interests, and are perplexed about how it could apply in a modern context. Many (43 of 161 respondents) to the online survey thought Te Tiriti should not be considered in the management of .nz and nine respondents thought all people should be treated equally in the management of .nz with no “special treatment” for Māori or due to Te Tiriti.<sup>146</sup> Some want to see greater involvement from Māori in the management of .nz and some consider the principles of Te Tiriti could be embedded in the approach to privacy, data protection, intellectual property and responses to abuse.<sup>147</sup>

UMR informed the Panel that the focus group participants consistently failed to see the connection between Te Tiriti and .nz (even the Māori participants).<sup>148</sup>

Despite stakeholders’ mixed views, the Panel believes these important issues must be more fully considered and solutions developed during our next phase.

### **Protecting te reo Māori in .nz domain names**

The Panel recognises the potential for te reo Māori to be used in the .nz domain name space in ways that are offensive to Māori. For example, any registrant can apply for the use of a domain name in te reo Māori. There are no requirements in the .nz policies to vet such an application to ensure it is used in a culturally respectful manner. This can result in the appropriation of te reo Māori in .nz domain names in ways that could cause offence.

Te reo Māori words could be misused by being, for example:

- used outside their cultural context
- spelt incorrectly, including the inconsistent application of macrons

---

<sup>145</sup> The Department of Internal Affairs (DIA) guide is an example: DIA, ‘The Kia Tutahi Relationship Accord Engagement Guide: Supporting Government Agencies to engage effectively with citizens and communities’, August 2016, [https://www.dia.govt.nz/vwluResources/Kia-Tutahi-Engagement-Guide-WORD/\\$file/Kia-Tutahi-Relationship-Accord-EngagementGuide2016.docx](https://www.dia.govt.nz/vwluResources/Kia-Tutahi-Engagement-Guide-WORD/$file/Kia-Tutahi-Relationship-Accord-EngagementGuide2016.docx)

<sup>146</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 29, [https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results\\_%20analysis%20and%20insights.pdf](https://internetnz.nz/sites/default/files/2.1%20dotnz%20survey%20results_%20analysis%20and%20insights.pdf)

<sup>147</sup> Ibid., 29–30.

<sup>148</sup> UMR, ‘Public perceptions of policy review for .nz: A qualitative study- focus groups’, p. 32–33.

- used with associated content that is offensive to Māori; and
- used in a way that is offensive to the special meaning and cultural significance of the words to Māori.

One point of comparison is the New Zealand Trade Marks Act 2002. This Act bars the registration of a mark which would be offensive to a section of the community including Māori. It also establishes an advisory committee to assess the trade marks offensive to Māori. Issues about the use of te reo Māori words for purposes other than for Māori benefit were the subject of a claim considered by the Waitangi Tribunal (the Wai 262 claim).<sup>149</sup>

The Panel found views were stronger in support of the protection of te reo Māori specifically.<sup>150</sup> Over half of respondents to our survey considered it important to protect the appropriate use of te reo in managing the .nz domain space.<sup>151</sup> Our research also provided feedback about what did matter in terms of protecting te reo Māori. Many suggestions were around ensuring the correct use of te reo Māori and providing protections around the management of applications for te reo Māori domain names.<sup>152</sup>

UMR informed the Panel that, in the focus groups, participants generally thought it is appropriate to protect te reo in certain cases. Yet, there was no strong endorsement to limit the general use of te reo because it was noted it is an official New Zealand language.<sup>153</sup>

The Panel observed .nz policies allowed for the use of macrons in domain names. Many Māori words require macrons to ensure they have the correct meaning and pronunciation. The Panel was advised by InternetNZ the use and application of macrons in Māori words for .nz domain names could be inconsistent. Some websites use the non-macronised version of Māori words, others do not. This is likely because no process exists for ensuring the proper use and protection of te reo Māori in .nz domain names. There is scope therefore for Māori-specific domain name abuse.

---

<sup>149</sup> Waitangi Tribunal, 'Ko Aotearoa Tenei: Report on the Wai 262 Claim Released, New Article, July 2011, <https://www.waitangitribunal.govt.nz/news/ko-aotearoa-tenei-report-on-the-wai-262-claim-released/>

<sup>150</sup> InternetNZ Secretariat, '.nz survey: p. 31; UMR, 'Public perceptions of policy review for .nz: a qualitative study - In depth interviews', p. 6, 12.

<sup>151</sup> InternetNZ Secretariat, '.nz survey results: p. 5.

<sup>152</sup> InternetNZ Secretariat, '.nz survey: p. 31; UMR, 'Public perceptions of policy review for .nz: a qualitative study - focus groups', p. 11, 33; UMR, 'Public perceptions of policy review for .nz: a qualitative study - In depth interviews', p. 6, 12.

<sup>153</sup> UMR, 'Public perceptions of policy review for .nz: A qualitative study- focus groups', p. 32-33.

The Panel was informed it is expected that the ability to register domain names with macronised characters was not widely known or understood, and InternetNZ did not provide guidance on how to appropriately use macrons for te reo Māori domain names. This is an issue because it not only allows for the misuse to occur, but also does not provide for recourse to ensure misuse can be rectified.

CIRA advised the Panel that the French equivalent of macrons, the five French accents, had been adopted into the Canadian domain system in 2012 with CIRA's launch of IDN domain names.

### **Protecting the use of Māori.nz and iwi.nz domain names**

The Panel has identified potential misuse of the Māori.nz and the iwi.nz domains specifically. Our engagement work did not identify this as an issue. However, the Panel felt these specific domain names warranted investigating because they were the only Māori specific second level domains approved by InternetNZ.

Māori.nz can be used by anyone who applies, while iwi.nz is regulated for use by Māori organisations only. This is an inconsistent policy approach. This is likely to be creating confusion in understanding the value of each of these 2LDs, and potentially could be affecting uptake. The Panel does not know how big an issue this is but considers it requires further investigation and seeks wider submissions on it.

### **Lack of culturally appropriate provisions in .nz policies**

The Panel is considering how often Māori views are catered for in the .nz policies. Our engagement work did not identify this as an issue but our reviews of the policies observed this gap. For example, the .nz Dispute Resolution Services policy provides the evidence required to have an unfair registration of a domain name.<sup>154</sup> There are no provisions if a domain name has been used in a culturally inappropriate way. Nor is there any provision for resolving disputes that encapsulate tikanga Māori practice for issues involving specific interest to Māori.<sup>155</sup>

Similarly, in the .nz Policy Development process document, there are no provisions for the appropriate design of policy that takes into account the interests of Māori as a priority group. Nor does the process document include any policy on how to properly engage and seek out the views of

---

<sup>154</sup> Clause 5 of the Dispute Resolution Services policy, <https://internetnz.nz/dispute-resolution-service-policy>

<sup>155</sup> Part B of the Dispute Resolution Services policy.

Māori in the consultation section.<sup>156</sup> The Panel considers these matters require further investigation and seeks submissions on these aspects during the next consultation phase.

The Panel notes this issue is relevant for other ethnic communities in New Zealand, as identified in the human rights section above.

## **Early thoughts**

The Panel believes InternetNZ policies do not provide the clarity needed to demonstrate the importance of Māori interests or provide for the required protections to uphold Māori interests. Greater reference and consideration of Māori interests within the principles and .nz policies is needed.

New Zealand would be taking the lead on this issue globally. Other equivalent international organisations<sup>157</sup> to InternetNZ have given only limited consideration to indigenous rights.

The Panel is aware that responding appropriately to Māori interests is complex. However, there are limitations to what issues the Panel is able to identify. The Panel can view issues for Māori taking into account its own views (provided by Maori specialists on the Panel) and views provided through feedback. However, it is conscious to effectively incorporate Māori interests, more engagement with a wider cross-section of Māori is required by InternetNZ as part of its broader review.

The Panel's view is the Internet and the .nz domain space are important tools for the commercial growth of Māori businesses and to enable Māori to connect in ways that were previously unavailable, as identified in the growth section below. The Panel believes the benefits of catering for Māori interests in the management of the .nz domain space could play a critical role in supporting tino rangatiratanga (self-determination) of Māori, position InternetNZ as a world leader in providing for the rights of indigenous peoples in ccTLD policy and make InternetNZ a more modern and responsive organisation in the bicultural New Zealand context.

---

<sup>156</sup> Clause 5 of the Policy Development Process, <https://internetnz.nz/nz-policy-development-process>

<sup>157</sup> Other similar regimes include Australia (.au), Canada (.ca) and the United Kingdom (.uk).

## **Growth: enhancing the .nz market place**

### **Definition of growth**

Growth is defined as value creation fairly distributed across society creating opportunities for all. This draws from OECD work<sup>158</sup> which has also fed into the New Zealand wellbeing budget approach.<sup>159</sup>

This section considers issues that may be limiting benefits to be gained from the .nz space in the areas of e-commerce and wider New Zealand enterprise. It also considers the operation and competitiveness of the existing .nz market.

### **Background**

The Panel recognises the .nz domain name space has created enormous community, social and economic growth as well as other benefits for New Zealand. A positive and growing .nz environment can add to the New Zealand economy by enabling businesses to reach a wider market. But .nz also strengthens communities and the wider society by creating connections and social growth.

During the Panel's consultation, there was strong feedback received indicating .nz policies should support business and that .nz needs to be more creative and innovative.

The growth area is strongly linked to the access and openness sections.

### **Issues identified**

#### **Opportunity for greater creativity, innovation and value growth within .nz**

The Panel found more creative and innovative options need to be worked through to better support New Zealand businesses and to grow value in the .nz domain name space.

The Panel considers further steps are required to better support .nz business activity. Most respondents to the online survey thought .nz policies should be used to help New Zealand businesses develop (52%

---

<sup>158</sup> OECD, 'Inclusive growth', <http://www.oecd.org/inclusive-growth/>

<sup>159</sup> Treasury, 'The Wellbeing Budget 2019',

<https://treasury.govt.nz/publications/wellbeing-budget/wellbeing-budget-2019>

think it is important or extremely important).<sup>160</sup> The Panel would like to further explore this. It notes CIRA has a statement in its vision on innovation.<sup>161</sup>

The Panel considers barriers may exist in the .nz domain name space that limit economic and social growth and opportunities. This is partly based on feedback provided to the Panel from UMR that lowering barriers to access generally for people is important, but also for businesses specifically. Barriers raised included:

- the perceived necessary skill level to register a .nz domain name
- lack of awareness and knowledge about the market and its benefits
- a lack of information about the role of InternetNZ and .nz in New Zealand
- preferred .nz domain names are not always available
- uncertainty over who are trusted registrars and what the cost should be
- uncertainty about the role of .nz and its ability to support growth
- perception you need to live in New Zealand to register a .nz domain name.<sup>162</sup>

Although access to .nz was generally thought of as good in the online survey, business respondents (together with government respondents) had the highest negative response rate (15%) to the online survey question asking if the people who need or want to access .nz have access to it.<sup>163</sup>

It is discussed above under “openness”, but from a growth perspective, a clear value case for a New Zealand geographic or comparable requirement to register and operate a .nz domain has not been established. The feedback generally supports or expects .nz domains to have a New Zealand base.<sup>164</sup> However, the RAG report did not support this given the mature market and a value rationale for building greater value by doing so has not been substantiated.<sup>165</sup>

The feedback shows a .nz domain name is considered a constraint for businesses with global ambitions unless selling something niche that is

---

<sup>160</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 35.

<sup>161</sup> CIRA, ‘CIRA’s vision for the future’, <https://cira.ca/internet-vision>

<sup>162</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 7-8, 10, 12, 13, 38, 41; InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 3.

<sup>163</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 20-22.

<sup>164</sup> UMR, ‘Public perceptions of policy review for .nz: a qualitative study- focus groups’, p. 9-10, 38.

<sup>165</sup> Registrar Advisory Group, ‘Response to the Initial briefing for .nz Panel from InternetNZ’, (unpublished), November 2019, p. 8.

closely affiliated with New Zealand like manuka honey.<sup>166</sup> A .nz email address is seen as not transferable but that it holds value in terms of security.<sup>167</sup> gTLDs are perceived to be cheaper, easier and better for global branding.<sup>168</sup>

Based on stakeholder feedback, the Panel sees merit in exploring the .nz domain name space to see if there are opportunities for greater innovation and growth.

## **Improvements to enhance market operation**

Enhancements to the way the market (and its participants) operate should be examined to ensure the roles are clear and the market structure enables optimal growth in the .nz domain name space.

The Panel found data on customer segmentation and penetration and excluded groups is absent. This made it challenging for the Panel to understand how big the problem is. Further research and engagement is required.

## **Registrants are not empowered**

An independent regulatory review by David Pickens in 2019 found registrants do not have the incentive, capability or capacity to engage in a way that drives better performance (best practice) from registrars or the operators of TLDs<sup>169</sup> It goes on to cite how important it is for consumers in a market to be able to influence producers (principally registrars in the .nz market) to deliver best practice.<sup>170</sup>

The review found Registrants have a poor understanding about how the domain market operates and who is responsible for what.<sup>171</sup> (This echoes the results of the online survey, Nethui session and research findings by UMR.) Registrants may also not fully understand the terms and conditions

---

<sup>166</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 37.

<sup>167</sup> UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 15-18.

<sup>168</sup> Ibid. p. 22., UMR, 'Public perceptions of policy review for .nz: a qualitative study- focus groups', p. 29-30.

<sup>169</sup> DNCL, 'Regulatory Review: prepared by David Pickens', August 2019, p. 28, <https://dnc.org.nz/sites/default/files/2019-08/Pickens%20Report%20-%20Independent%20Regulatory%20Review%202019v0.1.pdf>

<sup>170</sup> DNCL, 'Regulatory Review: prepared by David Pickens', August 2019, p. 28, <https://dnc.org.nz/sites/default/files/2019-08/Pickens%20Report%20-%20Independent%20Regulatory%20Review%202019v0.1.pdf>

<sup>171</sup> DNCL, 'Regulatory Review: prepared by David Pickens', August 2019, p. 28.

they sign up to with registrars. A registrant has not provided meaningful consent if they do not understand the terms and conditions.

A .nz principle states registrant rights come first - the rights and interests of registrants are safeguarded. However, the above examples indicate that this principle is not being fully reflected in existing operations. The Panel agrees registrants are relatively dis-empowered in the market unlike other comparable markets (eg. retail electricity, Ultra Fast Broadband) where consumer preferences and status are more visible.

The Panel would like to further consult to develop workable solutions to address these issues.

### **Resellers are not visible in the market**

The Panel considers the lack of regulation of resellers in the .nz domain name space results in little to no visibility of them and an inability to hold them to account for inappropriate or harmful activities.

The .nz policies place weight on openness in the market but the Panel has found opaqueness around the activities of resellers. Certain data about registrants is publicly displayed. However, the Panel has found little to no data on resellers. This does not align with the spirit of the policies, particularly with the principle that registrants should be protected.

The lack of visibility may also lead to a lack of enforcement of resellers and potentially higher rates of non-compliance. The DNCL reports regular policy violations by resellers including not allowing registrants to transfer and not making them aware of their rights. If a reseller has not complied with the .nz Operations and Procedures policy, the registrar may not always be able to hold the reseller to account. It depends on the individual contract terms between the registrar and reseller. This could in certain cases place too much accountability on registrars and not enough responsibility on resellers. The Pickens' Report also commented that there could be better enforcement of the standards on resellers.<sup>172</sup>

The RAG agrees there is a lack of transparency around resellers and their activities.<sup>173</sup> The RAG considers it is not only a problem for the registry but also registrars do not have a clear picture of how many resellers they have

---

<sup>172</sup> DNCL, 'Regulatory Review: prepared by David Pickens', August 2019, p. 36.

<sup>173</sup> Registrar Advisory Group, 'Response to the Initial briefing for .nz Panel from InternetNZ', (unpublished), November 2019, p. 4.

due to the lack of definition of a reseller and registrar platforms being inconsistent with how resellers are dealt with.

No criteria is provided in the policies on who can be a reseller. The policies do not require a reseller has particular credentials. Trade Me, for instance, requires a validation/registration process for all buyers and sellers.

The Panel would like to consult on this area to gauge the size of this issue if that is possible.

### **Registrars not incentivised to enhance market competition**

The Pickens' Report found no evidence of registrars using market power to the detriment of consumers (registrants). However, it commented that registrars are not engaging strongly with registrants. Registrars have commented there is opportunity for the registry to incentivise registrars to increase innovation potentially through flexible pricing and/or rebates against wholesale fee.<sup>174</sup>

Fewer active registrars may create less choice for registrants and possibly higher prices. The Panel would like to explore if this is an issue and whether increasing registrar numbers in New Zealand would create healthier market competition. A total of 90 registrars manage 710,000 domains in the .nz market. The UK has 2,500 registrars for 13 million domain names. CIRA has about the same number of registrars as .nz (about 100) for 2.8 million .ca domain names.

The Pickens' Report further commented that it should be easier to transfer registrants from one registrar to another.<sup>175</sup> The Panel would like to consult on this issue to gauge the size of the problem.

---

<sup>174</sup> Registrar Advisory Group, 'Response to the Initial briefing for .nz Panel from InternetNZ', (unpublished), November 2019, p. 1, 4.

<sup>175</sup> DNCL, 'Regulatory Review: prepared by David Pickens', August 2019, p. 36.

## **Registry too constricted in market**

The Panel considers the registry's role may be too constricted. It did not find any compelling case for the registry to have a direct sales relationship with registrants (and by-pass or compete with registrars).

The RAG report states it does not support InternetNZ communicating with registrants for anything other than compliance relating to New Zealand domain name policies.<sup>176</sup> It sees no benefit in the registry contacting registrants for any verification of contact details. It considers this should pass through registrars.

However, in meeting CIRA, the Panel found it provides registry products directly into the market. The .nz registry appears to have products it wishes to get to market. Options for it to achieve this need to be evaluated (eg. registrar incentives) to see if it is an issue.

As set out in the security section above, the policy disallowing the registry to contact registrants directly without the express approval from registrars may impinge on enhancing security of .nz and it could also restrict market growth. The Panel understands registrars are wary of the registry contacting its customers other than for policy compliance matters. Registrars have invested to attract customers and therefore want to protect these business assets. However, there may be other situations where the registry could benefit from making direct contact with registrants.

## **Barriers to grow .nz market for e-commerce**

The ease of access to good web development products is seen as important to e-commerce potential. The Panel found 60% of respondents said there were no barriers to using .nz. However, 33% did not know - 27% of this audience use .nz for business use.<sup>177</sup> This statistic is seen as not good enough. The cost to actually utilise .nz was identified as a barrier (including setting up a website where Panel feedback referred to the challenges for some in establishing an online presence). This was instead of establishing a .nz domain for which no significant barriers were identified in the Panel's survey work (for those who have internet access).<sup>178</sup>

---

<sup>176</sup> Registrar Advisory Group, 'Response to the Initial briefing for .nz Panel from InternetNZ', (unpublished), November 2019, p. 3-4.

<sup>177</sup> InternetNZ Secretariat, '.nz survey: summary and analysis'.

<sup>178</sup> InternetNZ Secretariat, '.nz survey: summary and analysis'.

Feedback on InternetNZ’s survey from 2018 found the key reason businesses chose another domain over .nz was cost. Also, the key reason businesses said they had not bought a .nz domain name yet was lack of knowledge about how to do it.<sup>179</sup> A further concern from the survey results impacting on potential e-commerce and the market is the number of businesses considering using .nz in the future had declined from 53% in 2014 to 46% in 2018.<sup>180</sup>

## **Second level market growth opportunities**

Global domain name registration growth is slowing, including in New Zealand.<sup>181</sup> The Panel wants to explore whether allowing greater expansion of the second level domains hierarchy for .nz, currently generally restricted, will contribute to greater value through more choice and better reflect New Zealand’s diversity. A potential example could be to create and allow registrations under “family.nz” to give individuals the opportunity to create custom domains for their families.

The Panel recognises there may be issues to be carefully considered around a second level market and conflicted domain names.

In Canada, CIRA supports domains at the second level.<sup>182</sup> Canada’s 10 provinces and three territories all have second level domain names eg. Ontario (.on.ca), British Columbia (.bc.ca). Although CIRA stopped registering new second level domains on October 12 2010, second level domains which were registered prior to that date are grandfathered and continue to be supported by CIRA.

---

<sup>179</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 8.

<sup>180</sup> InternetNZ Secretariat, ‘.nz survey: summary and analysis’, p. 24.

<sup>181</sup> Domainpulse, ‘As global TLD growth slides, 100 of top 300 TLDs contract: CENTR’, <http://www.domainpulse.com/2019/09/06/global-tld-growth-slides-centr/>

<sup>182</sup> Wikipedia, <https://en.wikipedia.org/wiki/.ca>

## **Next steps**

The Panel will now turn to developing options to address the issues it has identified with the .nz policies to help improve the .nz domain name space for New Zealanders.

It will engage the Internet community and wider public on these options in March/April of this year and use that feedback in making its recommendations to the InternetNZ Council by July 2020.

We embrace your thoughts and feedback as we continue our research, analysis and thinking for this review.

If you are interested in staying abreast of our work, you can follow the Chair's monthly blog on the InternetNZ website.

## Appendix: the roles of .nz market participants

Key participants who operate in the .nz domain space include the Registry, Registrars, Resellers and Registrants and each have distinct roles:

- **the Registry** – InternetNZ is the registry and has a number of key functions. Its main responsibility is to maintain and operate a central registry that holds all the information about .nz domains. The registry also provides associated technical services such as the Domain Name System (DNS) to facilitate delegation of registered domain names to registrants. The registry sets domain name prices, domain name policies and authorises registrars to resell domain name services on its behalf. InternetNZ created a subsidiary company, DNCL, which independently regulates the compliance of registrars, resellers and registrants with the .nz policies and deals with domain name related disputes. The registry receives a wholesale monthly fee from registrars for domain name registrations and renewals.
- **Registrars** – Registrars are authorised by the Registry to sell domain names. Registrars are responsible for marketing domain names and typically also sell attached products such as web hosting, email hosting to customers. New Zealand has approximately 90 registrars and about 710,000 .nz domains under management. Registrars have to operate within the .nz policies or face sanctions.
- **Resellers** – Resellers resell domain names and other services. They are typically contracted by registrars. These contracts are not standardised across the domain name industry. Resellers need to adhere to the .nz policies also. Registrars have a mix of IT systems and contract approaches to support resellers.
- **Registrants** – Registrants hold domain names and have a commercial relationship with registrars. Registrars are obligated to ensure registrants agree to adhere to the registries' policies when registering or renewing domain name licenses.
- **Regulator** - DNCL is the independent regulator of the .nz domain name space keeping .nz fair for everyone.