### Your details

|  |  |
| --- | --- |
| Name | Edwin Hermann |
| Email address |  |
| Contact phone number |  |

I understand and agree that my submission will be made public on the InternetNZ website

I understand that my contact details will be redacted from the public version of this submission

I would like to speak to my submission with the Panel

## Guiding Principles

|  |  |
| --- | --- |
| 4. | What would be the main benefits and disadvantages of moving from a ‘no concern for use’ approach to a ‘secure, trusted and safe’ approach? |
|  | I have a number of concerns with the idea of moving away from a “no concern for use” approach which I address below:  **Unnecessary**  The more regulation you seek to implement, the more difficult your job will be to determine whether you have got the balance right and the more time you will have to spend dealing with nuanced issues that arise from that.  By attempting to police and resolve these issues you will necessarily have to throw a lot of additional resources. This seems unwise and unnecessary.  **Duplication of Effort**  In many cases, existing law, practices and precedents already exist that deal with issues related to moving way from “no concern for use”. For example, if someone is hosting illegal material on a website, we already have a legal framework, and a number of government agencies already in place to identify, take action, and ultimately resolve the situation. Why would you want to try to duplicate this? It seems as though you would be re-inventing the wheel and there’s no reason to do so.  **Inconsistencies**  Furthermore, any policies you put in place that address issues in areas already covered by existing legislation or law enforcement agencies, you are likely to introduce inconsistencies. For example, two trademarks names may legally coexist (and may even have been tested in court) yet it’s entirely plausible that your rules may not allow the holder of one trademark to register it as a domain because it’s too similar to another domain name held by the other trademark holder. This would be incredibly frustrating for business and individuals alike.  **False Sense of Security**  The more regulation you place on the use of domain names, the more people will start making assumptions and give them a false sense of security. I think we all agree that .nz (or any domain space for that matter) would be better off without harmful use. However, introducing a whole raft of rules and policies around the use of domain names will certainly give people a false sense of security. Moderated 2LDs provide people with security and assurance, and rightfully so. People can be certain that, for example, a .govt.nz website will be owned and operated by a bonafide government organization and therefore will almost certainly not be a harmful site. But attempting to set rules around the use of .nz domains will be nowhere near watertight, therefore, unlike the moderated 2LD example above, people will falsely assume that .nz is generally safe.  **Summary**  In closing, I submit that a far better approach would be to retain the “no concern for use” model, but partner with enforcement agencies and other industry bodies. Work closely with them and establish bi-directional communications.  The banks don’t just freeze accounts as they please. NZ Post don’t confiscate parcels themselves. Storage providers don’t just turf people’s gear out. All these organisations work with government organisations and law enforcement agencies, such as Customs, MPI, NZ Police, the SIS, the GCSB, InterPol and the DIA. They maintain communication channels with these authorities, and refer matters to them for investigations to take place and/or action to be taken. It is only on instruction from those authorities that any revoking/cancelling/freezing take place.  In line with that, my suggestion is that you ought to retain the “no concern for use” model, and combine that with the establishment of a much closer working relationship and open lines of communication with relevant authorities. Ultimately this is better for everyone, and does not impinge on anyone’s freedoms. |

|  |  |
| --- | --- |
| 7. | Do you think there should be a new principle on te reo Māori and Māori participation in .nz? Why / why not? Do you have any comments on the proposed formulation of the new principle? |
|  | Use of Maori language should be encouraged and your systems and policies should facilitate this. However, any such policies should not come at the expense of freedoms elsewhere.  To give you an idea of what I’m referring to, allowing the use of macrons is an example of an initiative that directly supports the use of Maori language, and has no negative effects elsewhere. I support it for those reasons.  However, suppose you were to introduce a policy that dictated that macrons are compulsory for domain names with Maori words (or the opposite: no macrons can be used unless it is part of a Maori word), that would unnecessarily restrict freedoms to others (whether they are Maori or otherwise) and does nothing per se to directly support the goal of facilitating the use of Maori language. |

|  |  |
| --- | --- |
| 11. | Do you think the ‘first come first served’ principle should be modified and retained as an operational guideline? Why / why not? |
|  | The first come first served principle should remain.  It concerns me that you are considering, as stated in the Options Report, introducing a list of banned words (words that cannot be registered as part of a domain name).  Freedom of speech and freedom of expression is not only a human right but a value our society holds deeply. This is the case for pretty much all free and democratic countries.  Banning words is a direct attack of freedom of speech and freedom of expression and should not be tolerated. It is shallow-thinking at best, and a dangerous and slippery slope at worst.  All it will do is contribute to the erosion of freedom of speech that many western countries are seeing (e.g. cancel culture, political correctness, compelled speech bills), and it does not solve any issues.  New Zealand is a free country, a democratic country, a progressive country. Let’s reflect that in the way in which you mould your policies. |

|  |  |
| --- | --- |
| 14. | Do you agree that the ‘no concern for use’ principle should be modified and retained as an operational guideline? Why / why not? |
|  | “No concern for use” should absolutely remain. DNCL and InternetNZ should not be the judge and jury when it comes to the use of a domain name.  Instead, InternetNZ should establish close working relationships with law enforcement agencies and related authorities, such as the SIS, GCSB, the Police, DIA, InterPol, etc.  The problem with your proposed wording in the Options Report (page 31) is that it is far too vague to lead to any consistent interpretation. |

## Accessibility and openness of .nz domains

|  |  |
| --- | --- |
| 19. | Do you agree with our assessment of the options? Why / why not? Are there viable options that we have not mentioned? |
|  | What are you trying to achieve? If you are trying to achieve a greater access for people who do not speak English, then neither of the options you have suggested will address this.  You have missed a third option, which *will* address this, as follows:  Make the policies available in English, and take measures to add other languages over time according to how many people don’t already speak any of the languages in which the policies are currently available.  The reason that Option B does not achieved this lies in the fact that all (adult) speakers of Maori language also speak English, as quoted by Dr Peter J Keegan (<http://www.maorilanguage.info/mao_lang_faq.html>). Therefore, offering the policies in Maori would not increase access at all, not by even a single person.  Instead, you should use data from the Census to determine, *of the NZ population that does not speak English*, which language is next most commonly spoken. It is clearly not Maori (as per above), but instead likely to be Samoan, Northern Chinese or Hindi. This process can be repeated to gradually increase access to a greater and greater proportion of the New Zealand population. |

|  |  |
| --- | --- |
| 21. | Do you agree with our assessment of the options? Why / why not? Are there viable options that we have not mentioned? |
|  | There is a fourth option that you have not considered: Support any character that is encodable using Punycode.  All your other options limit the choices available in some way. It is not clear why, nor what advantage this provides over supporting all characters.  Allowing any character (provided it is encodable using Punycode) would provide the most choice, the most freedom, and the meet the needs of as much of the population as possible. |
| 22. | Which option do you prefer? Why? |
|  | I prefer the fourth option as per my response to Q21, where any character that is encodable in Punycode is allowed, because this provides the greatest flexibility.  However, of the options put forward in the Options Paper, I would prefer Option C because it provides the most flexibility, and best reflects the multicultural nature of New Zealand. Additionally, the advantages outlined in the Options Report for this option also far outweigh the disadvantages. |

|  |  |
| --- | --- |
| 23. | Which option do you prefer? Why? |
|  | Either Option A or B.  The solution to the problem of many people thinking .nz domain names are only registrable by NZ entities is best addressed by education, not by policy changes. |

## Security and trust

|  |  |
| --- | --- |
| 26. | Which of these options do you prefer? Why? |
|  | Option B.  InternetNZ should not be the arbiter on what constitutes illegal use. In the same way that banks don’t freeze accounts because they suspect there is illegal activity take place; these matters are instead referred to the law enforcement agencies. NZ Post don’t confiscate parcels simply because they suspect there is an illegal substance being imported into the country; they refer the matters to Customs and/or MPI.  Domain name registrations should operate in a similar way. To achieve this, InternetNZ should establish close working relationships with law enforcement agencies such as the Police, DIA, SIS, GCSB, InterPol, MPI, etc.  Option C is also a good option, provided the “trusted notifier” is a government agency, and not some third-party organization or private company. There would be too much risk of manipulation or corruption should “trusted notifier” include private organisations. |

|  |  |
| --- | --- |
| 28. | Which of these options do you prefer? Why? |
|  | Option A.  While your intentions came from a good place, in hindsight it would seem that introducing the interim policy was a knee-jerk reaction.  InternetNZ should not be the judge and jury over what constitutes illegal use. This should be left up to the law enforcement agencies that already exist to do this.  The correct way to tackle this problem is to establish good communications with these agencies, not by assigning yourself powers that leave its execution open to abuse. In the same way that banks don’t freeze bank accounts and NZ Post don’t confiscate parcels unless a government agency or a court order instructs them to do so, the same principle should apply here. To address the issue of expediency, establishing close working relationships with good lines of communication is key. |

|  |  |
| --- | --- |
| 30. | Which of these options do you prefer? Why? |
|  | Option B.  This is a well-thought-out option because it helps make .nz more trust and secure, and yet in doing so does not impinge on anyone’s freedoms or rights.  Unless the cost is prohibitive, this option should be given the greatest consideration. |

## Conflicted domain names

|  |  |
| --- | --- |
| 40. | Which of these options do you prefer? Why? |
|  | For Self-Conflicted Domains: Option B  It seems pointless for self-conflicted domains to continue to remain conflicted. This option is a pragmatic solution to the problem.  It is also a solution that does not favour one registrant over of another.  The disadvantage identified in the Options Report which talks about registrants not understanding the issues and how to resolve them can easily be addressed by communicating with these registrants.  Therefore, option B stands out as the best option. |

## Enhancing privacy across the .nz domain name system

|  |  |
| --- | --- |
| 44. | Which option do you prefer? Why? |
|  | Option B.  Option A is not ideal because while it takes a passive approach to privacy. Many people are not aware that registration details are (by default) visible on the Internet, and it would be extremely difficult to address this by education because the problem exists the moment someone registers a domain.  Option C is not ideal because it takes away a registrant’s choice to have their details visible. We should not assume that all individuals want their details withheld. There are situations where they may wish to have their details shown, e.g. they may be wanting to sell the domain name and would welcome contact from prospective buyers.  Therefore, option B is the best option because it provides the most flexibility whilst taking an active, and not passive, approach to privacy. |
| 45. | Under the IRPO, which contact details do you think should be withheld from WHOIS? |
|  | Registrant name, physical address, and postal address should be withheld.  The ability to withhold other details such as email address and phone number should be implemented as a per-domain option. |

## The .nz domain space and Māori

|  |  |
| --- | --- |
| 48. | Do you agree that following the Panel’s work, InternetNZ should take reasonable steps to engage with Māori when amending the .nz policies? Why / why not? |
|  | It is important to engage with Maori but this should not be done at the expense of engaging with the wider New Zealand public. All views matter.  I encourage InternetNZ to develop an engagement strategy with Maori, but to also include wider engagement to ensure that feedback from all sectors of society is sought. |