Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109 – 111 Featherston Street
Wellington, New Zealand
P +64 4 474 7590 F +64 4 474 7595
E enquiries@privacy.org.nz
0800 803 909 Enquiries
privacy.org.nz

28 August 2020

Sue Chetwin
Chair
.nz Policy Advisory Panel

By email only to: dotnzreview@internetnz.net.nz

Tēnā koe Sue

Office of the Privacy Commissioner submission on .nz Policy Review (Our Ref: P/1961)

The Office of the Privacy Commissioner welcome the opportunity to provide a submission on the .nz Policy Review. We are supportive of a robust .nz domain space that is accessible and privacy enhancing.

We understand the .nz Policy Advisory Panel is consulting on a refresh to the guiding principles and policy for the .nz domain space. Of key interest to us is the Domain Name Registration Data Query tool. Domain Name Registration information currently takes an open by default approach to registrant data. Individual registrants can request that their details be withheld from the database under the Individual Registrant Privacy Option (IRPO).

The comments below relate to the 'enhancing privacy across the .nz domain name system' the verification of applicant data, and the role of InternetNZ in providing a 'safe' place.

Enhancing privacy across the .nz domain name system (Questions 41 – 47)

We consider that the purposes for collecting registrant data is the primary issue that should drive the Panel's consideration privacy issues in the review. This is consistent with the approach of the Information Privacy Principles in the Privacy Act 1993.

Clearly articulating the purposes for which registrant data is collected will assist in answering the discussion paper's questions. We are mindful that issues such as the guiding principles being considered for the .nz domain space may influence the purposes for collecting registrant data and considering whether it should be publicly available. For example, a 'secure, trusted and safe' principle could mean that registrant data is more tightly held than currently (or conversely, that it is publicly available to provide for public scrutiny).

We recommend the Panel seek further information from InternetNZ and the DNZ. Specifically, information relating to the relationship between transparency and accountability and public access to registrant data, as well as complaints or concerns raised regarding public access to registrant data.

We are aware that making registrant data publicly available can create privacy risks. For example, screen scraping of WHOIS functionality can be used to create reverse lookup systems. The Panel should consider whether the benefits of public access outweigh the privacy risks presented.

Level of registrant data collected and stored (Questions 41 - 42)

The level of registrant data collected and stored should be consistent with the principles of necessity and proportionality expressed in the Privacy Act. The Panel should clearly articulate purposes for which information is required and then the data elements necessary to fulfil this purpose. With respect to the options presented, if more information than is currently necessary is being collected, then this should be addressed with a view to collecting less.

We agree with the assessment of the options in this section. However, we consider that the disadvantage of Option A (more individuals personal information publicly available) can be mitigated through the options discussed in questions 43-47. For example, having the IRPO chosen option by default. The Panel should consider the relationship between all of the options identified in questions 41-47.

Registrant data made public be default (Questions 43 - 45)

Making registrant data publicly available means that the domain name registry is a public register (albeit one without a statutory basis). There should be a specifically identified public interest that justifies public access to the information. This public interest could form part of the purpose of collecting the information. Any information made public would therefore be what is necessary for that purpose.

In general, we are supportive of keeping WHOIS as a public register of registrant details as an important transparency and accountability measure. We can see the purposes for which the information is made public could range from allowing for website owners to be contacted about problems with their website, to allowing for public scrutiny of who is operating a website (similar to the companies register). The Panel should discuss these and any other purposes in more detail.

We need further information to understand the public interest that the Panel considers is being serviced. The wide difference between the options in this section suggest potentially different public interests could be served. For example, Option B (individual registrants have the IRPO by default and would need to opt out from it) suggests that the personally identifiable information is not that useful for transparency and accountability purposes – while the current state suggests that personal information is important to the public interest.

Implementation of the IRPO and access to registrant information when required (Questions 46-47)

Where personal information has been withheld, InternetNZ provide a process so that it can be accessed upon request. Additional work is needed to understand why this information should be available upon request when it is not typically available, what tests are applied to any release, and how these purposes differ from those considered in questions 44 - 45 above.

In general, we support Option C, which would allow registrants to be contacted through an online form without requiring the publication of a registrant's details. However, additional information is needed on this issue.

Verification (Questions 29 - 30)

We understand that there can be domain name registration abuse but that this is only addressed in a reactive manner. We support Option B at page 55 - introducing data validation for all domain name registrations. It is our view that applicant data should be validated before the application is granted. This is consistent with Information Privacy Principle 8 of the Privacy Act, which requires that reasonable steps are taken to ensure that personal information is accurate, up to date, complete, relevant, and not misleading.

Data such as contact details for the applicant should be verified to reduce the risk of the applicant not being contactable in the event of an incident. For example, requiring verification emails to be sent.

Data such as the proposed domain name should be validated against a restricted character set. This would reduce the risk of homographic compromises and is consistent with Information Privacy Principle 5.

InternetNZ's role in providing a 'safe' place

We understand that Panel recommends developing a 'secure, trusted and safe' guiding principle for the .nz domain. We agree that the .nz domain should be secure and trusted. We consider that the 'safe space' principle could significantly change InternetNZ's role and responsibilities. This change could mean that InternetNZ becomes an arbitrator of activity within .nz domains. We are keen to understand what this role would look like in practice and whether the Panel anticipates a change in the collection or use of personal information than in order to fulfil this new function.

We trust that you find the above submission helpful as you consider the review of dotNZ. We are mindful that this Office was unable to engage with the advisory team earlier in the year due to the COVID-19 general lockdown. We would greatly appreciate further engagement with the team before decisions are made.

Ngā mihi

Liz MacPherson
Assistant Commissioner, Policy and Operations