



7 June 2016

Debbie Monahan
Domain Name Commissioner
Domain Name Commission Limited
PO Box 11-881
Wellington 6142

Dear Ms Monahan,

Review of the .nz WHOIS service

Thank you for the opportunity to comment on the proposed suppression process for personal information on the .nz WHOIS.

The current position of the DNC is that all .nz registrant information is public. The DNC has proposed a new process to withhold an individual's contact details in some circumstances.

In our previous submissions on .nz WHOIS policy, we advocated that WHOIS information should not be accessible in cases where personal privacy outweighs the public interest in making that information accessible.

We also suggested that Domain Name Commission (DNC) consider the public good of making individual domain registrants' information available. If the public good argument is not strong, an alternative approach would be to offer an opt-in/out choice to registrants.

While the register of .nz domain owners is not an official "public register," it has many of the hallmarks of public registers. Public registers have privacy controls built into their individual legislation, as well as specific provisions in the Privacy Act. It is just as important to safeguard the personal information in the .nz register as it is with any public register.

Given overseas evidence of WHOIS data being abused^[1], or being used to compromise someone's online credentials^[2], it is our view that protecting the privacy of individuals may also serve other more general public interests such as consumer or community safety.

The proposed criteria

The DNC proposes that individuals need to demonstrate that their interest in withholding the information outweighs the DNC's need to make .nz WHOIS information public.

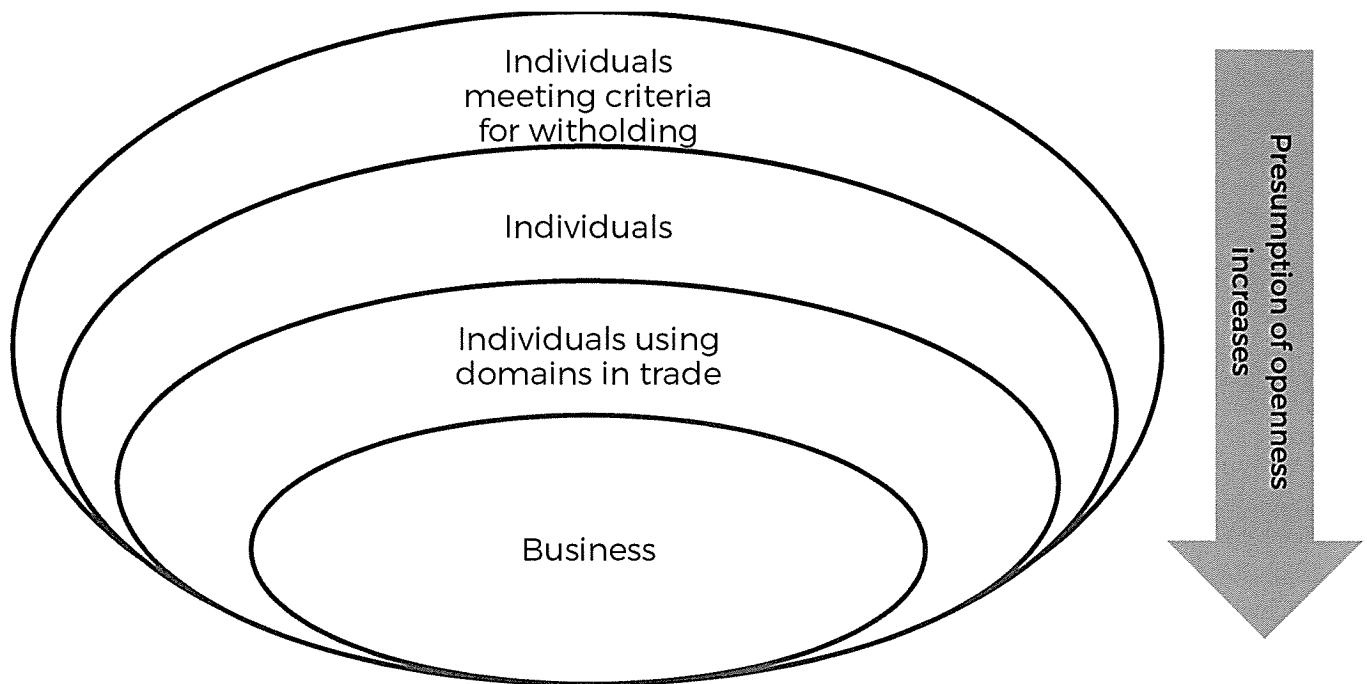
^[1] Letter to ICANN from the Online Abuse Prevention Initiative, July 2015 <http://onlineabuseprevention.org/letter-to-icann-july-2015/>

^[2] How Apple and Amazon Security Flaws Led to My Epic Hacking, Mat Honan: <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>, Amazon's customer service backdoor, 'Eric': <https://medium.com/@esprunge/amazon-s-customer-service-backdoor-be375b3428c4#.8txj30qqv>

An example situation would be where there are concerns for personal safety. Individuals would need to provide relevant supporting documents (protection, trespass or restraining orders for example) along with their application, as well as information about alternative measures that have or have not been taken to protect the information.

We recognise that, in most cases, ensuring access to the Register's information is an important public good and is necessary for the effective operation of the domain name system. However we consider that where an individual is under the protection of a legal order, the default position of openness may raise safety concerns or expose them to other potential harm.

In our view there is an increasing presumption of openness and a diminishing expectation of privacy as one moves from vulnerable individuals towards businesses:



The FAQ that the DNC has released makes it clear that the information collected is not intended to be onerous. However, in many situations, the information about alternative measures could be handled proactively. DNC material could provide those applicants with a list of potential measures they can take *in addition* to their application for suppression.

Process for consideration

The DNC's proposal will collect more information from individuals, specifically individuals that have expressed concerns that they are at risk or vulnerable in some way. Any collection of information should be supported by appropriate controls. To maintain public trust in the .nz Register, the DNC will need to demonstrate they have robust protections and processes in place. We recommend undertaking a privacy impact assessment process to establish how DNC will deal with this new information, and we are happy to support the DNC in this process.

When considering requests to disclose information that the DNC has suppressed on the .nz WHOIS, the first criteria applied should be whether the individual consents. Where that consent is not provided, the criteria to release or disclose information could be modelled on the Privacy

Act's Information Privacy Principles - namely Principle 11 which permits disclosure for a number of grounds, including to prevent or lessen a serious threat to individual or public safety, and to avoid prejudice to the maintenance of the law.

The DNC may be considering, in some cases, sensitive or traumatic information. Our investigations and dispute resolution teams have considerable experience in this field, and we are happy to provide assistance as needed by the DNC – whether in establishing the DNC's internal process for considering applications, or playing a role in the appeals process.

Transparency and trust

It is vital that the public trusts the .nz Register. To help foster this trust it is important that the DNC clearly communicates its position that .nz WHOIS information should be public to New Zealanders. We understand that this is a long-held position, but believe that there is value in raising awareness of the reasons behind it.


The DNC could elevate this discussion by explaining the public benefits and value that maintaining a transparent register brings. Having a widely understood position on this would make it clearer to applicants how decisions about suppressing their information are made, and what their personal interests are balanced against.

The DNC did not previously have a formal, published system in place for suppressing details, and this offers one. It is important that people understand how the DNC decides where to draw the line between individual privacy and public good – and that this position is convincing.

Another way to help build trust in the .nz Register would be transparency reporting. We recommend that the DNC consider some form of reporting on their decisions to release withheld .nz WHOIS information, in particular how often, to whom and the proportion of requests complied with.

We hope these comments and suggestions have been useful. If there is any further assistance we can offer as part of this process, please do not hesitate to ask.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'TH' followed by a stylized surname.

Tim Henwood
Senior Policy Adviser, Technology