Privacy Commissioner
Te Mana Matapono Matatapu

9 February 2016

Office of the Privacy Commissioner
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109-111 Featherston St
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

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 policy framework review.

Currently WHOIS information is made available by default. We suggest this should not be the case where personal privacy outweighs the public interest in making that information accessible.

In our submissions on the .nz policy framework in July 2015 and the stage one WHOIS service review in November, we gave the example of individuals protected under the Domestic Violence Act. Given overseas evidence of WHOIS data being abused[1], or forming the first piece in the puzzle of compromising someone's online credentials[2], protecting the privacy of individuals may also serve other more general public interests such as consumer or community safety.

Locally, similar registers have changed over the time since the New Zealand was established. In 2009 the Land Transport Act was amended to restrict access to Motor Vehicle Register (MVR) data. In addition to limiting the purposes for which MVR data could be used, it gave New Zealanders the option to not make their information available on the register.

We recognise that adding complexity and judgement calls to the process of maintaining the Register increases the cost of maintaining the Domain Name System. We also recognise the need to maintain the integrity of the DNS and the need to balance the ability to contact registrants against privacy interests.

We suggest that these considerations can be balanced to produce a mechanism for the Register to limit personal information provided through a WHOIS search where individuals attest that they have a heightened need to protect their privacy. Developing such a mechanism will enhance both the privacy and safety of individuals.

Our answers to the Domain Name Commission's policy questions are set out below:

---

[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/@espringe/amazon-s-customer-service-backdoor-be375b3428c4#.8txj30qgv

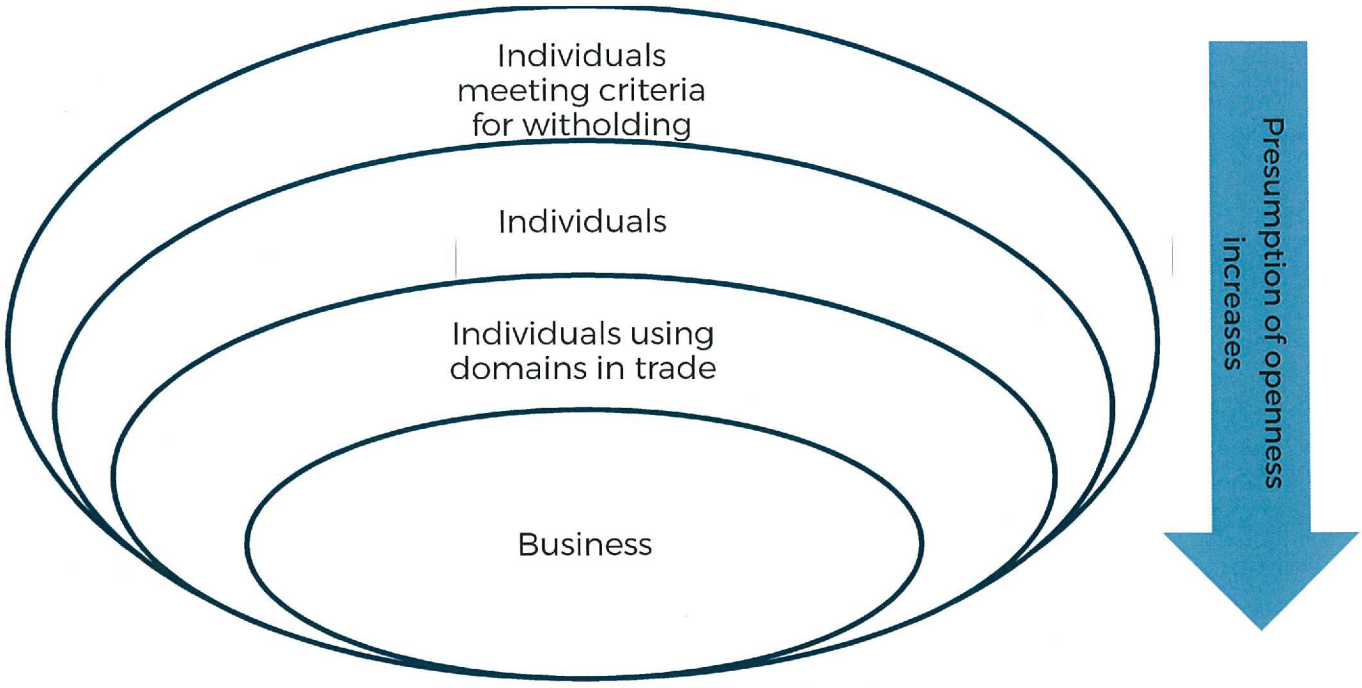
Should there be a different approach for registrants who are individuals over where an organisation is the registrant?

There should be a different approach for *some* registrants who are individuals, particularly where those individuals are vulnerable or require extra protection.

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. There is a strong public good in making the details of an organisation's domain registrant available, but the argument for making an individual's available is weaker given the potential for misuse. In cases 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.

To better understand the scale of the issue, we would be interested in any data or research DNC may have on the amount of individuals with registered domains compared with organisations.

In our view there is a increasing presumption of openness – or a diminishing expectation of privacy as you move along the spectrum from vulnerable or protected individuals to businesses:



Should there be a different approach for when the domain name is being used in trade, regardless of whether the registrant is an individual or an organisation?

Broadly speaking, if a domain is being used in trade, the registrant is going to be an "agency" under the Privacy Act. The approach used for domains registered by an organisation should have enough nuance to protect the privacy of individuals using domain names in trade.

Individuals in business choose to use different data in their transactions with different agencies. This is particularly important for sole traders, where there may be little or no distinction between what is business information, and what is personal information (for example, where a business is conducted largely from a residence).

For sole traders, administrative efficiencies may be reduced, and business costs increased, if they must go to additional lengths to ensure the effective separation of business activities they do not wish to have arbitrarily linked.

While individuals using a domain name in trade may wish to register their contact address as a PO Box or similar, rather than their residential address, having clear information available to help them make that call at the time of registration is important.

Should the registrant name always be shown but the contact details withheld in certain circumstances?

In certain circumstances, it might be appropriate to withhold registrant contact details. There may also be instances where it is appropriate to withhold the name of the registrant as well.

Any ability to suppress personal information should be flexible enough to respond to multiple situations. The Register has many of the characteristics of a public register, but because it is not recognised as a public register under schedule 2 of the Privacy Act 1993, it lacks many of the statutory protections a public register would have.

To be clear, we are not advocating that the Register become a public register, but given the role the DNC plays and the value of the data held in the register, we believe it would benefit greatly from the inclusion of a similar suppression mechanism. Many of those suppression mechanisms include withholding names as well as contact details.

Should registrants be able to hide their identity behind a proxy registration?

We do not currently have a view on what the suppression mechanism for Register data could be, but a proxy service is one possibility.

However, as discussed below there may be other options that remove the requirement for a proxy service.

If any data is withheld from publication on a WHOIS record:

What information should be withheld?

Information should be withheld where release is not in line with the purpose of collection, or where there is another, overriding privacy interest in withholding it. An overriding privacy interest would be a legal protection order, or some other evidence that releasing the information would compromise the individuals' safety or expose them to harm.

Withholding contact details, but providing some form of contacting the Registrant for administrative or technical reasons should suffice. The Registrant contact details will sometimes be the same as one or two of these categories, so in those cases it may make sense to withhold admin or technical contact details as well. A proxy registrar, or proxy contact point may be the appropriate mechanism for these situations.

What should be the criteria to withhold the information?

At the very least, DNC should consider offering a suppression mechanism to people who have or would be able to seek suppression on existing public registers. In many cases, those registers have criteria in place so looking to the administration of those registers may be useful. Some examples would be the rating information databases kept by local authorities or the unpublished electoral roll mechanism.

DNC should also consider the public good of making individual domain registrants' information available. If DNC finds that the public good argument is not strong, an alternative approach would be to offer an opt-in/out choice to registrants.

Who should decide if a name meets those criteria?

Individual registrars could make these decisions provided there was a central set of criteria and guidelines for their application provided by DNC.

It may also be beneficial to set up some form of appeal process – if a registrar declines to suppress an individual's contact information, the DNC could reassess the application.

What should be the criteria to enable the withheld information to be released?

The first criteria applied should be whether the individual consents. Where that consent isn't provided, the criteria to release or disclose information could be modelled on the Privacy Act's Information Privacy Principles - namely Principle 11 which concerns disclosure.

It is important that if there is a means to withhold information, that that mechanism does not frustrate existing access for legitimate purposes – for example contacting the Registrant with a takedown request under the Harmful Digital Communications Act.

Who should decide if an application to obtain the information meets those criteria?

If there are clear criteria this decision could be handled by registrars. It would ideally be supported by a transparency requirement to report on how often this information is released. If there is likely to be difficulty in applying the criteria, or considerable nuance is required, then having a single decision-making point such as the Domain Name Commissioner would aid consistency.

We do however recognise the additional complexity – and therefore cost - that this decision making would add to the maintenance of the DNS. Therefore the simpler and clearer the criteria can be made, the better.

If there is any further assistance we can offer as part of this process, please do not hesitate to ask.

Yours sincerely

Tim Henwood
Senior Policy Adviser, Technology