

2 February 2016

Debbie Monaghan
Domain Name Commissioner
Level 11
80 Boulcott Street
PO Box 11-811
Wellington 6142

By email: policies@dnc.org.nz

Dear Ms Monaghan

The .nz WHOIS Register – Review, Stage 2

Thank you for the opportunity to make a submission in relation to stage 2 of the review of the Domain Name Commission (DNC) WHOIS register.

The key question for stage 2 of the review is *whether the current range of data should continue to be provided for a WHOIS search on the same basis as it is now*. The WHOIS system generally works well and the Law Society has only a few recommendations for the Commission to consider:

- That the system should provide additional protection for personal privacy where possible. In particular, there should be a well-publicised mechanism for registrants to be able to **suppress** their personal information where publication puts their safety at risk.
- That the **identity** of domain name registrants should continue to be publicly available, to support the purposes and the integrity of the registration system.
- **Contact information** also needs to remain quickly and easily available for legitimate users. However, contact information provides a particular vector for misuse of the register. It is therefore worth considering whether it is possible to create a practical alternative to online publication.

The importance of maintaining the integrity of the domain name system

The domain name system is an integral part of modern commerce and also supports individual registrants' ability to exercise their freedom of expression online. It is essential that that system is trustworthy.

Unfortunately, misuses of the system occur from time to time. For instance, some people register domain names to mislead consumers, to circumvent their competitors' rights, to engage in identity theft or to attack other individuals.

When misuses occur, it is important to be able to deal quickly and effectively with them. Quick and effective enforcement reduces the financial, emotional and reputational damage that can occur. It also has a deterrent effect, though it will not stop misuses altogether.

Adjusting the system to provide better privacy protection

The current registration system operates on the basis that all registration information is always

available online. While this has the advantage of simplicity, there is no accommodation for legitimate individual privacy concerns. It is possible and desirable to create a more nuanced approach.

As previous submitters have pointed out, online publication can cause real harm to registrants including:

- Publication of personal information can create serious risks to safety, particularly for people who are victims of domestic violence or similar levels of threat.
- Details can be used to engage in scams, phishing attacks, identity fraud or other criminal activity.
- Details can be used for the purposes of spamming.
- Details are also used for marketing activities that fall outside the purposes for which the registration system exists.

The Law Society recognises that the New Zealand domain name system sits within the context of international domain name management. Effective protection cannot be achieved with purely on-shore solutions. However, as a small domain registration system, it may be possible for New Zealand to consider a new way of operating that fulfils the purposes of the register while providing some additional protection for privacy.

The key concern – suppress details where there is evidence of risk

The Law Society recommends that the WHOIS system should be altered to permit suppression of personal information where there is evidence of risk to personal safety.

There are existing precedents for this approach. Several other New Zealand public registers allow for suppression of details from online publication where there is a protection order in place (for instance the electoral roll, and the motor vehicle register).

Under section 115 of the Electoral Act 1993, the name and certain other details of a person may be exempted from publication on the roll, or from inspection, if the Electoral Commission is satisfied, on the application of any person, that the publication of that person's name would be prejudicial to the personal safety of that person or his or her family. Evidence that may be provided in support of such an application expressly includes (without limitation):

- a copy of a protection order that is in force under the Domestic Violence Act 1995, or
- a copy of a restraining order that is in force under the Harassment Act 1997, or
- a statutory declaration from a member of the Police to the effect that he or she believes that an individual's personal safety, or that of the individual's family, could be prejudiced by the publication of the person's name.

The ability to suppress will only be effective if individuals are aware that it exists. If the Domain Name Commission introduces a suppression mechanism, the Law Society recommends that the Commission publicise its availability.

The Law Society's remaining comments about publication of identity and contact information refer to situations where there is no evidence of a risk to personal safety.

Continue to publish identity of registrants online

It is possible that making a registrant's identity publicly available (with no contact information) could

lead to harm to that individual. However, the risks are relatively low. In contrast, the benefits of publication of identity appear to be relatively strong.

Publishing the identity of registrants provides a deterrent to malicious or improper domain registrations. It also allows for more effective dispute resolution.

In particular, the identity of the registrant is usually key in considering whether a registration is unfair or intended to mislead. Complainants therefore need to know the identity of the offending registrant before they can receive effective advice about their legal options. They also need to know the identity of the offending registrant before filing a complaint, so they can make the strongest possible argument. Complaints may be dealt with 'on the papers', without an opportunity to present further information.

Publication of registrant identity appears to be a reasonably necessary and effective way of supporting the registration system.

Requiring registrants to disclose their identity may be a barrier to expression for some people. Section 14 of the New Zealand Bill of Rights Act 1990 is therefore a relevant consideration. However, as already noted, there are sound justifications for disclosure of identity in this context. Registrants who wish to protect their identity also have easy access to alternative offshore registration systems or other online products and services that allow for anonymity.

As a result, publication of registrant identity does not appear to be an unreasonable or disproportionate limitation on expression. It may even enhance rather than discourage legitimate commercial expression. It supports the aims of the domain name registration by allowing registrants to communicate with each other effectively, support their trademarks, deter malicious or bad faith registrations, and support the dispute resolution system.

The pros and cons of taking contact information offline

There is an argument from a privacy perspective that contact details for individuals should only be available on request, rather than being made available automatically online (as is currently the case with the WHOIS register). However, the issue is whether it is practical and proportionate to take registrants' contact information offline.

The need for easy access to contact information

It is vital to ensure that those with a genuine need to contact a registrant are able to obtain contact information without delay or unreasonable cost.

There are many legitimate reasons for making a registrant's contact information quickly and conveniently available. A few examples include:

- Contacting a registrant for lawful reasons, (for instance to purchase a domain name, or to communicate information that may benefit the registrant)
- Communicating with registrants who may have registered an unlawful domain name (either unintentionally or in bad faith)
- Taking legal action against bad faith registrants or registrants who have engaged in other unlawful conduct.

The current system of publishing all contact information online is a simple and effective means of ensuring that legitimate access to contact information is maintained. It is instant, highly efficient and cost-effective.

However, it is worth considering whether there are equally practicable alternatives that would protect privacy better.

The privacy perspective

Contact information is valuable for identity fraudsters, spammers, scammers or others engaging in criminal activity. It is also valuable for those who want to engage in legal but potentially unwanted and annoying activities such as marketing.

Currently, there appear to be no technical, contractual or practical barriers to using information from the register for purposes that are different from the purpose for which the register exists. This unrestricted approach to the register contradicts the normal approach under New Zealand privacy law. Personal information should generally only be used for the purposes for which the register exists, unless one of a limited number of exceptions apply. For instance, use of information for court proceedings will always be acceptable, but use of information for marketing purposes falls outside the reason for which the register exists.

Misuses of information can undermine trust and confidence in the register as well as creating real risks for individuals.

Of course, individuals can take steps to protect themselves as long as they are aware that information is going to be published online. However, as a general principle the burden for protecting privacy should not fall entirely on the individual. A central principle is that individual privacy should be protected to the greatest extent possible without the individual needing to take action.¹

A practical compromise?

Improvements in technology create options that may not have existed when the current registration system was created. These may make it practical to remove contact information from public view, but to make it available to legitimate requesters quickly and cheaply.

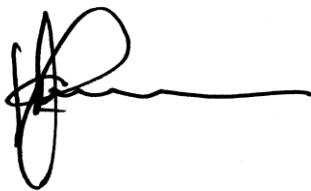
One example is to establish an online request system (with protections against harvesting of personal information) that allows legitimate requesters to receive registrants' contact details instantly. Such a system would create an audit trail of searches, which could deter misuse. Requesters could be asked to verify that their search corresponds with one of the listed purposes for which the register was established.

An existing and well-regarded model for this in New Zealand is the Personal Property Securities Register.

Conclusion

This submission was prepared with assistance from the Law Society's Human Rights & Privacy and Commercial & Business Law Committees, and we hope the comments are useful to the Commission. If further discussion would assist, please do not hesitate to contact the Law Society's Law Reform Manager Vicky Stanbridge (vicky.stanbridge@lawsociety.org.nz / 04 463 2912).

Yours sincerely



Chris Moore
President

¹ "Privacy by design": <https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf>