

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

Attention: Debbie Monahan

6 November 2015

Email: policies@dnc.org.nz
VIA EMAIL ONLY

Your Ref:

Our Ref: DEK 167138NZMS

Dear Debbie

Contacts:

Baldwins Intellectual Property
Review of the WHOIS Service by the New Zealand Domain
Name Commissioner

Penny Catley - Team Leader,
Partner
Deborah Kessell-Haak – Senior
Associate
Anna Bargh - Associate
Alex Coats - Team Administrator

We refer to the request for submissions in relation to the review of the current WHOIS policy and how it operates.

The following constitutes submissions made on behalf of Baldwins Intellectual Property.

Executive summary:

This submission, in summary, supports the continued collection and publication of WHOIS data. It also proposes that those collecting the data be responsible and accountable for its accuracy. We suggest that the interests of privacy would, in most cases, be more usefully protected by technical means than by allowing anonymity. The principal reasons behind our submissions are as follows:

1. Domain names are economically important as a valuable intellectual property right, and as a means for New Zealand enterprises to conduct business.
2. Misuse of domain names or websites associated with domain names is a serious legal and commercial issue.
3. The WHOIS system must allow the owners of trade marks and other intellectual property rights to identify those misusing domain names to enable those owners to properly enforce their legal rights.
4. This important function of the WHOIS system is undermined by:
 - a. Toleration of inaccurate WHOIS data;
 - b. Permitting some domain name registrants to remain anonymous for alleged privacy reasons.

This letter and any accompanying documentation may contain privileged and confidential information. If you are not the intended recipient, your use of this information is strictly prohibited.

5. Collectors of WHOIS data are best placed to ensure that it is accurate and that any alleged need for privacy is substantiated before anonymity is granted. Enforceable accountability mechanisms would incentivise data collectors to meet these standards.

Background - Intellectual Property and the Online Environment

Trade marks

Products and services are, in general, best known by their associated trade mark. For this reason, it is common practice for trade mark owners to incorporate their trade mark into the domain name of a company's home website. It is important for companies to include their trade mark within a domain name as it is by this trade mark that consumers distinguish the products or services of one company from those of another on the internet.

The domain name registration process has created serious legal issues pertaining to trade marks. Unlike the rules set out in the Trade Marks Act 2002 (NZ) and other similar legislation throughout the world, the rules for registering a domain name do not include any procedure to ensure that a requested domain name is not infringing upon a previously registered domain name or trade mark. As a result, not only is it very easy but it can be very profitable for a registrant to register a domain name that includes a trade mark to which the registrant has no rights.

Registration and use of a domain names in violation of trade mark rights can occur in a variety of ways. These include the registration of the trade mark or common misspellings of the trade mark as a domain name. This results in internet traffic being directed away from the business of the holder of the trade mark to an unrelated website and/or damage to the reputation that adheres to the trade mark.

Counterfeit products and other IP infringements

In addition to the registration and use of the domain name itself as an infringement, websites linked to specific domains can be used as a means of promoting and selling goods and services that infringe a whole range of intellectual property rights. These include the promotion and sale of counterfeit goods or goods that may otherwise infringe patent or design rights, engaging in conduct that would constitute passing off, that is misleading or deceptive or would amount to a misrepresentation, and the use of copyright works and trade marks within a website.

In addition to the sale and promotion of these goods and services being to the detriment of rights holders, often such sales also incorporate a health and safety aspect. For example, the increasing sales of counterfeit medicines¹, electronics, cosmetics, and children's toys raises significant safety concerns.²

Legitimate Interest

The holders of intellectual property rights have a valid right granted to them under common law or by statute. They are, therefore, as entitled as users of the domain name system ("DNS") to

¹ Ministry of Health, *Counterfeit Medicines – Don't Fake Concern*, June 2005, available at <http://www.medsafe.govt.nz/profs/particles/counterfeit.htm> last accessed 3 November 2015

² New Zealand Customs Service, *Fakes – What's The Deal?*, Contraband Magazine, Issue 126, Autumn 2014, available at <http://www.contrabandmagazine.org.nz/issue/cover/126>, last accessed 3 November 2015; see also Jason Wall, *Customs NZ seizes more than 43,000 counterfeit goods in 2014*, NBR Online, available at <http://www.nbr.co.nz/article/customs-nz-seizes-more-43000-counterfeit-goods-2014-jw-167335> last accessed 3 November 2015.

have their concerns regarding infringement in an online context addressed. Currently, the WHOIS service is the only means for rights holders to effectively achieve those ends.

Concerns regarding the Current Approach

We have opted to respond to this question first as the concerns with the current approach largely determine how the WHOIS system should be managed in order to address those concerns. In our opinion, concerns regarding the current WHOIS approach fall into the following broad categories: purpose, privacy/transparency, accuracy, accountability.

Purpose

We argue below that the function of the WHOIS database should be expressly acknowledged to include a law enforcement/protection purpose. Once the purpose is defined, the rules and mechanisms that should be put in place to support that purpose become clearer.

In our opinion, debate regarding the particular concerns surrounding the WHOIS database has been stymied because the purpose or function of the WHOIS database has never been accurately defined.

A country's top level domain is often viewed as a flagship of a country's internet participation and as a strategic asset with economic, socio-economic, internet stability and security implications.³ Management of country-code TLDs were originally delegated in order to allow local internet communities to develop their own locally responsive and accountable DNS services. The guiding principle in policy making at ccTLD level is that ccTLD policy should be set locally according to national law.⁴

Given the above, therefore, there is both a need and opportunity for the purpose of the WHOIS service as relating to .nz to be expressly defined. Once defined, it becomes easier to determine what rules should be put in place and where the onus for ensuring those rules are complied with should lie.

For example, if the collation of registrant data is deemed to be purely for technical purposes in relation to the technical maintenance of the DNS then very minimal contact data need be collated and the accuracy of the data would be important but not critical (other mechanisms being available to ensure technical stability). In turn, the onus of ensuring accuracy of the data could reasonably be placed on the provider of the data as there is no gain in them providing inaccurate information. Privacy concerns would also outweigh the need for transparency as only a registry would need contact details for the above purpose.

If, however, an acknowledged purpose of the collation of the data is also to preserve the .nz ccTLD as a strategic asset, to maintain stability and security and to enable the appropriate enforcement of national laws in the online environment, i.e. a protective function, then the level of data collated must increase and the accuracy of the data becomes paramount. This is because, as discussed below, the information will be needed to identify the holder of the .nz domain in order to allow rapid and effective enforcement. In addition to all the above, if enforcement/protection is an acknowledged purpose, then a balancing exercise would also

³ See OECD Working Party on Telecommunications and Information Services Policies, *Evolution in the Management of Country-Code Top Level Domain Name (ccTLDs)* (DSTY/ICCO/TISP(2006)6/FINAL; 17.11.2006), available at <http://www.oecd.org/sti/ieconomy/37730629.pdf>, last accessed 5 November 2015

⁴ Bylaws for Internet Corporation for Assigned Names and Numbers, Article IX, Section 4(10), available at <https://www.icann.org/resources/pages/governance/bylaws-en/#IX>, last accessed 31 October 2015.

need to be undertaken with privacy considerations being weighed against the importance of the protective or enforcement function of the WHOIS service.

Privacy/Transparency

We argue below that privacy concerns must be balanced as against legitimate interests in the transparency and accessibility of the WHOIS data. In addition, we argue that there is a net social gain in maintaining and further promoting access to WHOIS data

The issues that are central to the argument in favour of stronger privacy considerations can be divided into three main categories: mass solicitation, individual targeting and suppression of political and social discourse. The mass solicitation issue is based on a concern that the data will be used for marketing purposes such as spam, mass mailings and telemarketing.⁵ The individual targeting category is very broad but includes use of the information collated for purposes such as identity theft or stalking. The final category of concern is based on the theory that anonymity promotes political and social discourse because it provides the 'speaker' with protection from retaliation. In contrast, the concerns of intellectual property rights holders are narrower but equally important. Essentially, rights holders are concerned to have a means to identify and locate infringers in order to enforce validly held rights granted by common law and statute.

We argue, however, that the needs and concerns of intellectual property rights holders and those seeking privacy protections are not mutually exclusive. Requiring and enforcing accurate and accessible WHOIS information along with the implementation of robust accountability mechanisms has a net gain for privacy protection. Intellectual property rights holders will benefit by having a reliable source of information they can use to protect such rights. Personal information, although required to be true and accurate, will be protected because parties intending to use that information for illegal purposes will not be able to hide behind a veil of anonymity. The law abiding consumer will benefit from being able to gain accurate information that can be used to contact the domain name holder.

Instead of limiting access to the information, therefore, the balancing act between protecting privacy and ensuring that the online environment is safe and beneficial to all can be better protected by applying technical solutions to prevent misuse, ensuring that those using the WHOIS service lose their ability to be anonymous and ensuring that accountability mechanisms for misuse are put in place and actively enforced.

In relation to the theory that anonymity protects political and social discourse and that requiring accurate and accessible WHOIS information would have a chilling effect on this discourse, we note that there are a limited number of websites that are within the scope of this argument and more than sufficient opportunities online (other than holding a domain and website) to enter into such discourse. In addition, complete anonymity is almost impossible in the 'real world' and, therefore, allowing complete online anonymity would give participants in such activity more protection than they are currently granted in the 'real world'. As such, any balancing act between such rights and having an accurate and accessible WHOIS database must fall in favour of accuracy and accessibility.

Accuracy

The accuracy (or lack of accuracy) of the information that can be obtained by way of the WHOIS system is a major concern for intellectual property rights holders.

⁵ See for example *Register.com, Inc. v Verio, Inc.* 126 F. Supp. 2d 238 (S.D.N.Y) relating to the use of automated bots to mine WHOIS data.

There are a number of domain name related protection and enforcement mechanisms available to intellectual property rights holders including the Trade Marks Clearinghouse, the Uniform Dispute Resolution Service, the Uniform Rapid Suspension System and the Domain Name Commission's own Dispute Resolution Service. In addition, rights holders may opt to take the matter of an alleged infringement of intellectual property rights through the New Zealand court system.

However, in order to both try to resolve any matter and to enforce any validly held rights, the perpetrator of the alleged infringement needs to be identified. The ability to identify and locate infringement offenders, especially repeat offenders, remains a major obstacle preventing the adequate protection of intellectual property rights in an online environment. Enforcement of intellectual property rights is often hampered as a rights holder using the WHOIS service is repeatedly faced with parties who have deliberately provided inaccurate information. If, therefore, the purpose of the WHOIS service is expressly acknowledged to have an enforcement or protection purpose, then it is important to ensure that the data collated is accurate.

As the provider of the information may have reason to provide inaccurate information in order to avoid identification, the onus of ensuring the accuracy of the data provided should not vest with them. Instead, the onus on ensuring the accuracy of the information should vest with the party having the means, funds and imperative to impose accuracy. We would submit that the appropriate party is the one that is collecting the information and deriving income from the registration system. They should, we submit, be required to institute proactive checks on the accuracy of information being provided. Mechanisms would then need to be put in place to ensure that this party was free to act in this capacity and to ensure that their compliance was actively monitored and enforced through appropriate sanctions.

Accountability

In our opinion, a lack of accountability for the proper management of the WHOIS service is a major flaw.

The current system makes the violation of intellectual property rights easy and the evasion of responsibility even easier through the provision of inaccurate data. We submit that the entities in charge of domain name registrations and WHOIS queries must start actively enforcing the contracts with registrants that are already in place requiring the provision of accurate and complete information and be made accountable if they do not.

Specific Questions Posed by the Commissioner

Why data should be collected

As argued above, the protective/enforcement function of the WHOIS system must be an accepted and expressly acknowledged purpose of the WHOIS system. Once this is acknowledged, we submit that it becomes essential that fully detailed and accurate information on .nz registrants must be collected to enable the fulfilment of that function.

Why data should be publically available

As argued above, an accurate and publically accessible WHOIS service results in a net social gain. Misuse of the data can be managed by having appropriate technical solutions and accountability mechanisms in place rather than limiting public access.

Why the display and availability of data should **mostly** be same for all parties

We consider that the default position should be that the display and availability of information should be the same for all users of the DNS system. If the appropriate technical and accountability mechanisms are put in place and actively enforced, then privacy concerns will be appropriately addressed without limiting the availability and display of the WHOIS data.

If, however, the user can show a valid reason why such information should not be displayed, then a mechanism should be put in place to consider and, if appropriate, enable such a request. Any such ability should be limited to those that can prove to the registrar that the display of information would be detrimental; for example, if they are an individual, hold a protection order and they cannot arrange for a third party (also under an accuracy/accountability obligation) to be the contact person and pass on any correspondence relating to the domain or the website.

We acknowledge that protection from overwhelming electronic solicitation due to the collation of WHOIS data by automatic means is warranted. However, we submit that the problem posed by such activity is best prevented by technical means (such as password protecting the database to prevent such access) as opposed to limiting access by 'type' or 'activity'.

Conclusion

For the reasons outline above we submit that at an absolute minimum the current system of the collation, display and grant of access to WHOIS data should be maintained. However, we also submit that there is a real opportunity to effectively define the function WHOIS service for the benefit of all users of the DNS. There is also a real need to improve the accuracy of the data and the accountability systems in place regarding the use and misuse of such data.

Further Submissions

As the next round of proposed consultation will be on what information is displayed and how, we have left our current submissions at a reasonably high level. We are very interested in being involved in the next round of consultation as we would like to present proposals on the actual mechanism that should be put in place to ensure that the WHOIS service remains an accessible tool for intellectual property rights holders but also balances the competing concerns detailed above. To that end, we would appreciate being informed as to upcoming public consultations.

Yours sincerely

Baldwins Intellectual Property



Deborah Kessell-Haak

Senior Associate

Direct Dial: (+64 4) 471 6884

Direct Email: Deborah.Kessell-Haak@baldwins.com