ANDREW BROWN
QUEEN'S COUNSEL

Andrew Brown QC, LLB(Hons)(Auckland), BCL(Oxon)
Bankside Chambers, 22nd Floor, 88 Shortland Street, Auckland
P.O. Box 2815, Shortland Street, Auckland 1, New Zealand
Telephone: 64-9-366 6139, Facsimile: 64-9-366 6140
Email: andrew@andrewbrown.co.nz
Website: www.andrewbrown.co.nz

6 November 2015

Debbie Monahan
Domain Name Commissioner
Email: policies@dnc.org.nz

Dear Debbie

SUBMISSION ON .NZ WHOIS REVIEW

1. Thank you for your letter dated 6 October 2015 inviting submissions regarding the review of the .nz WHOIS service.

2. I attach my submission to this letter.

Yours sincerely

Andrew Brown

SUBMISSIONS ON REVIEW

OF .NZ WHOIS SERVICE

5 NOVEMBER 2015

ANDREW BROWN QC

To: *policies@dnc.org.nz*

(1) The issue

1. The DNC is conducting a .nz WHOIS review. It has sought views on why there should be a .nz WHOIS service that makes available the information the DNC collects when registering a .nz domain name.

(2) Summary of position

2. The name and address of the registrant should continue to be publicly available in the same way as is the case with registration of companies, incorporated societies and trade marks.

3. Contact telephone and email details could be withheld to stop spam and unwanted targeting by marketers. However, if such details are to be withheld, there is a need for a mechanism whereby the DNC will make contact telephone numbers and email addresses available:

   (a) Where there is a need for law enforcement purposes;

   (b) Where there is credible evidence of a website being used to breach another party's rights and the complainant has attempted to contact the registrant by way of the physical address but has had no response within seven days.

(3) Discussion

4. It is submitted that .nz registrant data should be collected and should be publicly available for the following reasons.

   (a) Domain name litigation

5. Domain names are important to modern commerce. Businesses naturally seek registration of domain names that comprise or incorporate a name or trade mark in respect of which they have rights.

6. There are two important categories of situation which demonstrate the importance of registration data being publicly available.

   Wrongful acts conducted on website corresponding to domain name

7. A considerable number of domain name registrants, once they have registered a domain name, use the corresponding website for wrongful purposes. The wrongful purposes include selling counterfeit goods, distributing pirated copyright material or engaging in misleading or deceptive conduct and other breaches of the Fair Trading Act to the disadvantage of consumers.

8. In respect of such parties it is imperative for rights holders and competitors[1] to know who is the registrant of the domain name as well as contact details in order to be able to take action to protect rights. Any anonymity of registrants will simply add another layer of cost to rights holders taking action. Why should it be necessary for a rights holder to have to go the High Court (with all the added cost to obtain under the *Norwich Pharmacal* procedure) the name and address of a domain name registrant in order to be able to take action in the first place.

Bad faith registrants: DNC DRS service

9. Unfortunately it is not uncommon for a party unrelated to a rights holder to register and use a domain name with bad faith intent to profit from the goodwill of a rights holder. Disputes over such bad faith registrations are frequently litigated.

10. Since 2006, 334 complaints have been made under the Domain Name Commission's Dispute Resolution Service (DRS) in relation to .nz domains.[2] 94 of these were withdrawn, and 16 were dismissed. That means 224 complaints resulted in a substantive outcome for the complainant of cancellation, transfer or settlement (67%). Other cases have proceeded through the High Court.

11. As can be seen from the percentages of positive outcomes for complainants, the majority of complaints related to registrations found to be in bad faith.

12. The DNC DRS service provides complainants with an alternative to bringing court proceedings. For this alternative dispute resolution service to work, it is vital that a complainant be able to identify a registrant. Under the NZ DRS, a complainant, in order to be successful, must establish that the registration of the disputed domain name is "unfair". A number of the matters which the Dispute Resolution Service Policy states may be used as evidence that a domain name is an "unfair registration" require the complainant to know who the registrant is (e.g. paras 5.1.3, 5.1.4, 5.1.5, and 5.3 of the Policy). It is therefore imperative to the workability of the DRS that registrant data remains accessible.

13. Anonymous domain name registrations using "proxy registration" services are common in the .com domain space. Bad faith registrants frequently use these to hide their tracks. This adds an additional layer of cost, delay and complexity to a domain name dispute due to use of proxy services to anonymise registrants. This additional layer arises because the complainant has to send its complaint to the WHOIS-listed registrant of record (i.e. the proxy registration service). Sometimes the registrar or proxy registration service will disclose the underlying registrant to WIPO. WIPO then makes the underlying registrant information available to the complainant, and provides the complainant the opportunity to amend its complaint. It is likely that the complainant would do so, because to succeed the complainant must show that the domain name has been registered and is being used in bad faith. Clearly bad faith is more difficult to show in many cases without knowing the registrant's identity. (Very often bad faith is personal to the registrant rather than being something that can be asserted and proved regardless of the identity of the registrant.) The process therefore takes longer and involves more cost to the complainant than would otherwise be the case. It would

---

1 It is well established that the principal means of enforcement of the Fair Trading Act 1986 is through competitor activity.

2 See dnc.org.nz/content/infographic.pdf.

be undesirable if inefficiencies of this kind arose in the New Zealand context. They would be inevitable in the case of anonymous registrations.

14. The efficiency of the DRS alternative dispute resolution service therefore requires that accurate registrant data is collected and made available.

(b) Risk to free speech not outweighed by benefits of data collection

15. While anonymous free speech is valuable in certain situations, there are alternative methods to registration of a .nz domain name for those who wish to engage in anonymous speech. For example, an anonymous speaker could operate a blog or register a domain name in another jurisdiction where registrant data is not publicly accessible. The Protected Disclosures Act 2000 provides protection for employees who want to engage in legitimate whistleblowing activities, making anonymity less essential in that sphere.

16. Freedom of speech under s14 of the New Zealand Bill of Rights Act is not absolute. With freedom comes responsibility. There are a number of judicial and statutory controls on freedom of speech relating to protection of rights or reputations of others, protection of national security, public order, public health and morals.[3]

17. In this context, the benefits of collection and publication of registrant data are not outweighed by the risk that some individuals may have to find other avenues for anonymous speech.

(c) Cellphone numbers and/or email addresses are often the only reliable way to contact a registrant

18. I acknowledge the concerns of other submitters that the public availability of registrant contact information can have unwanted side effects e.g. targeting by marketers and spam. Misuse of email addresses and contact phone numbers can give rise to harassment. However, in circumstances where people often change their physical address without updating their contact details in relation to domain name registrations, cellphone numbers and email addresses can in practice be the only reliable means of contacting someone. This is because it is in an individual's interest to keep the same cellphone number or email address in order to keep in contact with friends, family and associates.

19. Because of the possibility of abuse in relation to phone numbers and email addresses in particular, I support the adoption of mechanisms to protect these details, while keeping registrant information such as name and address publicly available. Public availability of names and addresses is consistent with the Companies Office and trade marks register. Contact details of company directors are publicly available on the Companies Office website, as are address details for owners of registered trade marks on the Intellectual Property Office of New Zealand's site. A domain name is a valuable right, like a trade mark registration, so it is fair that, in exchange for the right, there exists a public record of the rights holder's details. However, the difference between the Companies Office and trade marks register records and

---

[3] See Article 19(3) International Covenant on Civil and Political Rights: "the exercise [of the right to freedom of expression] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order, or of public health or morals."

the .nz WHOIS service are that they do not make email addresses or contact phone numbers available.

20. However, it is also important that there is a mechanism in place whereby contact phone numbers and email addresses will be made available when there is genuine need to contact a registrant. To achieve this, a system could be set up whereby if phone numbers and/or email addresses are needed for law enforcement purposes, they are immediately available to a law enforcement officer on application to DNC.

21. In other circumstances, such as the making of a domain name complaint, or where there is credible evidence of a website being used to breach another party's rights, a phone number and/or email address could be made available to a complainant once he or she has attempted to contact the registrant by way of physical address but had no response within 7 days. Alternatively, DNC could set up a system whereby a person seeking to contact a registrant by email enters their message into a form on the DNC website, which is then forwarded to the registrant without disclosure of his or her email address. It is vitally important that there is such a mechanism available to permit access to contact information in the form of email or telephone where another party's rights are being infringed and attempts to contact the registrant via a contact address have been unsuccessful.

Andrew Brown QC