Australian Privacy Foundation

Submission to auDA on WHOIS Policy and Registrant Contact Information Policy Reviews

Prepared by: John Selby, Lecturer, Macquarie University

October 2010

Introduction

This document provides background on the review currently being undertaken by auDA of its WHOIS Policy and its Registrant Contact Information Policy. It briefly explains the historical context of the review before giving an overview of the six major issues being contested by various stakeholders. It describes those stakeholders and their motivations before giving a detailed perspective on each issue for consideration by the APF. Finally, it provides a draft APF submission to auDA on both policies.

History

For nearly a decade, auDA has regulated the .au domain name space. auDA is an industry self-regulatory body that operates subject to the imprimatur of the Australian government (which has legislative power to declare domain names as "electronic addresses" subject to direction by the Australian Communications Authority and the Australian Competition and Consumer Commission in the event that auDA becomes dysfunctional).

auDA operates review panels for its policies on a rotating basis. It seeks submissions from a variety of stakeholders and, after considering those submissions, then sets/adjusts its policies accordingly. auDA created its registrant contact information policy ("RCI Policy") in 2002 and its WHOIS Policy in 2006. The WHOIS policy prescribes what information about the registrant of a .au domain name will be collected, used and made available through the WHOIS service (a standard feature of the Internet since the invention of the domain name space has been the maintenance of a searchable database which enables interested persons to find out the details of the registrants of domain names). The RCI Policy prescribes what information is mandatory or optional for a registrar to collect from the registrant of a domain name at the time of registration of that domain name.

Issues

As auDA's WHOIS database is publicly accessible, there are a number of issues arising out of the WHOIS Policy and the RCI Policy which have privacy implications and over which stakeholders are contesting. These contests fit within two broad categories:

Scope of registrant identity disclosed:

1) Whether the actual names of domain registrants must be collected during the registration process and subsequently disclosed through WHOIS searches OR can the identity of re-sellers be used in the place of the name of the domain registrant;

2) Whether a registrant need only supply an email address relating to their position when registering a domain name OR their personal (ie named) email address;

3) Whether the date of registration and/or renewal of a domain name should be made publicly available through WHOIS searches;

Accuracy of registry identity disclosed:

4) Whether the registrar/reseller should rely upon the granting of a warranty by the registrant that their details are accurate OR whether the full contact details of a registrant should be verified by a registrar/reseller on the registration of a domain name;

5) Whether the registrant should be the sole entity to bear the duty to update their personal information when it changes OR whether the registrar/re-seller should bear a duty to take positive steps to remind registrants to update their personal information (and if so, how often?);

6) What the consequences should be if a registrant's personal information is not kept up-to-date (nothing/slap on the wrist/reminder notice/deletion of the domain name from the registry).

Stakeholders and their Positions:

- **Pro- strong IP Lobby / Law Enforcement**: A driving force behind the requirement for public access to WHOIS data, the pro-strong IP lobby (ie trade mark owners and their legal representatives, international IP organisations) desire full disclosure of verified personal information belonging to registrants so as to make it as easy and low cost as possible for themselves to track down and prosecute any domain registrant who might infringe on a registered trade mark. Similarly, law enforcement desire the ability to easily identify who to prosecute in the event the content hosted on a computer linked to a registered domain name violates the law of some country.

- **ISPs, Registrars and Re-sellers:** These entities desire low barriers to the registration of domain names so as to maximise the volume of registrations (from which they profit). Some ISPs/re-sellers desire the ability to insert their own contact information into the WHOIS database so as to make it more difficult for registrants to churn between ISPs/re-sellers. Other ISPs/re-sellers prefer only customer information so as to more easily attract churning customers.

- **The Australian Government:** Having outsourced the cost of developing Domain Name policy to auDA, the Australian Government seeks to minimise open conflict amongst the various stakeholders. The ACCC seeks to ensure that barriers to industry competition between registrars and re-sellers of domain names are minimised so as to foster vigorous competition between them. The Australian Federal Police support public disclosure of WHOIS information.

- **Australian Personal and Business Internet Users**: Internet users generally desire the ability to easily register a domain name at low-cost and to be able to transfer that registration to another registrar/re-seller/ISP with ease (if they so desire). Internet users do not want to be the recipients of spam, false/misleading marketing schemes or false/misleading domain renewal scams. Personal Internet Users may have very strong reasons for desiring anonymity or non-release of their entire personal information (eg a recently acrimoniously divorced spouse who gained custody of children may fear the use of WHOIS data by their ex-spouse to cause harm to them and/or their children). Australian Business Internet Users may desire the efficiency of only revealing the role of the person who registered a domain name (rather than that person's actual name) so as to avoid problems which can arise as a consequence of staff turnover / termination of email accounts belonging to former staff. To protect their

privacy, these users do not wish the marketers/spammers/fraudsters to gain the capability to fully and automatically search the WHOIS database.

- **Professional Domain Name Traders:** The limited re-sale of domain names having been permitted by auDA in recent years, these traders desire full disclosure of the personal information of registrants and the date of registration/renewal of domain names so as to reduce the cost of their marketing efforts to buy and/or sell domain names. They seek to lower barriers to re-sale so as to arbitrage the difference between the cost of registering a domain name and the potential value of that domain name to an Internet user who might actually use it for something more than click-through advertising.

- **Marketers/Spammers/Fraudsters:** These fringe groups (ab)use the WHOIS database as a source of targets for a variety of frauds: For example, they seek unfettered access to email addresses for the purposes of targeting spam and they seek unfettered access to domain registration/renewal dates so as to send fraudulent invoices to domain registrants. auDA has taken legal action against several of these groups, but they still persist and will seek to exploit any advantage they can that may be unintentionally crafted into the WHOIS Policy and/or PCI Policy.

Possible APF Positions

As a body dedicated to protecting the privacy of Australians, the APF might consider adopting the following positions on these issues:

Issue 1: Whether the actual names of domain registrants must be collected during the registration process and subsequently disclosed through WHOIS searches OR can the identity of re-sellers be used in the place of the name of the domain registrant?

There may be very sound reasons why an individual might want to avoid disclosing to the public their identity through a searchable database. Whilst the provision of accurate information to the entity to which that individual has entered into a contractual relationship so as to facilitate the registration of a domain name is beneficial, such information should not be made mandatorily available to any third party (eg: a trade mark holder or law enforcement agency) who might wish to undertake a WHOIS search. If that third party has a legal right to know the actual identity of the domain registrant, then a court order served on the registrar is a reasonable requirement.

From a competition perspective, it is important that domain registrants have the right to easily transfer their registration to another ISP/registrar/re-seller. Thus ISPs/registrars/re-sellers should only be able to insert their information into the WHOIS database in place of the personal information of a registrant with the express consent of the registrant (ie opt-in).

Position 1: The APF should support the existing right of domain registrants to not disclose their actual names through WHOIS searches. Domain registrants should retain the right to opt-in to having the identity of their ISP/registrar/re-seller listed.

Issue 2: Whether a registrant need only supply an email address relating to their position when registering a domain name OR their personal (ie named) email address?

There are sound reasons why a registrant might only wish to provide positional (not personal) information when registering a domain name. In particular, businesses of all sizes

face issues relating to staff-turnover and the danger of not receiving notifications if personal email addresses of their staff were to be required within the WHOIS database as opposed to the use of positional email addresses (eg: when Jane Doe quits as IT manager at Hero's Salami Factory and is replaced by John Smith, the owner of Hero's Salami would prefer to not have to update their domain registration to replace jane.doe@herossalami.com.au with john.smith@herossalami.com.au).

In pushing for the removal of the option of using positional email addresses from which the WHOIS database, trade mark holders are concerned only with transferring their own enforcement costs onto all other domain registrants. Such a change would not be an efficient solution overall for the Australian Internet community (ie compare the cost of every Australian domain registrant having to constantly update personal information in the WHOIS database vs the costs to trade mark holders in finding the identities of <35 domain registrants per year).

Position 2: The APF should support the existing right for domain registrants to supply positional email addresses and oppose any change which would require the disclosure of name email addresses in the WHOIS database.

Issue 3: Whether the date of registration and/or renewal of a domain name should be made publicly available through WHOIS searches?

There is significant evidence justifying the non-disclosure of the date of registration / renewal of domain names within the WHOIS database. This non-disclosure minimises the risk to Australian Internet users of falling prey to false invoice scams and un-intended ISP/registrar/re-seller churn which has occurred in the past.

Position 3: The APF should support the existing non-disclosure of the dates of registration and/or renewal of domain names so as to minimise the risk of fraud against domain registrants.

Issue 4: Whether the registrar/reseller should rely upon the granting of a warranty by the registrant that their details are accurate OR whether the full contact details of a registrant should be "verified" by a registrar/reseller on the registration of a domain name?

By seeking the verification of registrant details, trade mark holders are seeking to transfer their enforcement costs onto third parties. Australians are not required to have a licence to access and/or use the Internet and ISPs, registrars and re-sellers are not Australian government entities. Not all Australian Internet users have a drivers licence or passport. This should not be an Australian Identity Card by stealth. Registrars, ISPs and re-sellers do not have systems in place to undertake verifications and the cost of properly doing so (ie minimising false positives and false negatives) would far outweigh any benefits. This proposal is inefficient as it seeks to require hundreds of thousands of annual identity verification checks to be undertaken in an attempt to lower the cost of identifying the respondents to the approximately 35 .au domain name disputes lodged annually.

Position 4: The APF should support the existing requirement that registrars/re-sellers should rely only on the warranty by the registrant that their details are accurate and strongly oppose any requirements that registrant details be "verified".

Issue 5: Whether the registrant should be the sole entity to bear the duty to update their personal information when it changes OR whether the registrar/re-seller should bear a duty to take positive steps to remind registrants to update their personal information (and if so, how often)?

Trade mark holders again seek to transfer their enforcement costs onto ISPs/registrars/re-sellers through requiring the sending to registrants of annual/bi-annual reminders. Whilst ensuring the accuracy of information within the WHOIS database is important, the question is how (and to whom) the cost of doing that updating should fall. Trade mark holders and domain re-sellers would acquire the benefits of more accurate information whilst ISPs/registrars/re-sellers (and ultimately their customers, Australian Internet users) would bear the costs.

As more common updating is not particularly privacy intrusive (and has benefits through more accurate information), a possible compromise position would be for the trade mark lobby and domain re-sellers to pay for the costs incurred by registrars/ISPs/re-sellers in sending annual (or bi-annual) reminder emails to registrants. The implementation costs (and the willingness of those stakeholders to open their chequebooks to cover such costs) would have to be determined. No change to the status quo should be made until clear determination of those costs and stakeholder transfer payments occurs. One possible method of recovering the costs would be to increase the fee for lodging a domain name dispute (such disputes are usually lodged by trade mark holders). However, as only ~35 such disputes are lodged annually under the auDRP, the per-dispute fee increase would be likely to be quite substantial.

Position 5: Unless those stakeholders who would benefit from the transmission of reminder notices are willing to bear the costs incurred in sending those notices, the APF should support the position that the registrant of a domain should be the sole entity who bears the duty to update their personal information when it changes.

Issue 6: What the consequences should be if a registrant's personal information is not kept up-to-date (nothing/slap on the wrist/reminder notice/deletion of the domain name from the registry)

There are a variety of legitimate reasons why a domain registrant may not receive a notice from their ISP/registar/re-seller or a trade mark holder (eg: going on holidays, ISP data crashes, intervening spam filters, etc). It would be excessive and a denial of procedural fairness for a domain registrant to have their domain deleted from the registry simply for failing to respond to a notice. ISPs/registrars/re-sellers are not courts and should not be imposing such sanctions without properly granted court orders or auDRP decisions. Those ISPs/registrars/re-sellers should not be exposed to potential lawsuits from domain registrants for incorrectly terminating their registrations. The appropriate process for trade mark holders who cannot make contact with a domain name registrant is to seek such a court order or auDRP decision. This proposal is similar to the attempts by copyright holders to have ISPs act as their extra-judicial enforcement agents through "three-strikes" notices sent to Internet account users around the world and should be resisted just as strongly.

Position 6: the APF should support the status quo position of there not being specified sanctions for a registrant's failure to keep their personal information up-to-date