

Comments on WHOIS Policy (2002-06), June 2003

Mr Sam Johnston <samj@aos.net.au>

Director

Australian Online Solutions
94-98 Chalmers Street
Surry Hills NSW 2010
1300 132 809

Please consider the following comments when reviewing the WHOIS policy, which deal primarily with the .com.au 2LD and take into account technical, legal and consumer issues.

Collection of Information

Consumers should be able to map from a domain name to a responsible entity. Ideally entities would be identified by their correct legal name and Australian Business Number (ABN). This provides accountability for consumers and recourse for the victims of intellectual property abuses, trademark misuse, defamation etc. It also allows the registrars to identify exactly who they are dealing with. Other databases already exist for obtaining more detailed information about an entity (ASIC, ABR, White Pages etc.) and it is not necessary to replicate these databases. The amount of information collected should be minimised and despite the Privacy Act only applying to individuals ('natural persons'), I believe the cost of differentiating between individuals and other entities outweighs the benefit of providing more detailed information where permitted by the act. Furthermore, collecting more information than people are comfortable with providing will only cause contamination of the database.

Unique Identifiers

Where possible, ABNs should be used to identify registrants (especially for the .com.au TLD). If and only if an ABN is not available, other identifiers may be considered, including ACNs and Registered Business Numbers. As it is possible to conduct a business as a sole trader or partnership without an ABN or business registration it may be necessary to use the correct legal name of the registrant alone in some cases.

Verification of Information

Information provided by registrants should be at least sanity checked, but ideally verified automatically at the registry level against existing database(s). I do not know of any test like the credit card luhn check which enables users to

verify the various government issued unique identifiers. I cite the explorer.net.au interface as a good example of a system which verifies registrant data without creating an undue administrative effort for the registry, registrar or registrant.

Updating of Information

As this information may change over time it should be verified again on renewal. The positive side effect of this is that within 2 years the database will be forced into a more consistent state and the expense of doing so will be distributed across the registrants.

Strong Authentication

There is no requirement for strong authentication and I believe it is important that registrants can progress from searching to live in as short a period of time as possible. Extra administrative checks provide little in the way of security and are expensive to implement. x.509 certificates are a better way to solve the problem of authentication and the cost of verification is borne by the registrant. The existing legal system has mechanisms to deal with fraudulent activity. Furthermore, domains with incorrect information should be subject to deletion (with appropriate notification/resolution periods of course), assuming they are not already.

Individuals' Domain Names (.id.au)

While it may be necessary to identify the entity responsible for a commercial web site there may be advantages in restricting access to information for .id.au domains. Publicising this information adds little value and restricts individuals' freedom of speech by denying users anonymity (which they will otherwise obtain elsewhere anyway) at the expense of accountability. In the absence of a system to prevent users from furnishing false information I believe publishing this information is only likely to cause contamination. This information would still be available through legal channels (eg. for defamation proceedings) and the responsible person could still be contacted via email (eg. for serving of take down notices).

Disclosure of Email Address(es)

Email addresses should continue to be disclosed. Not only does this allow users to contact the entity responsible for a domain (be it for outage notification, take down notices etc.), but it also enables registrants to check that their information is up to date and verify where key requests will be sent. Hiding this information will cause problems for registries and registrants alike and I believe the benefit of disclosing it outweighs the cost. There are technical

measures available to reduce SPAM and domain related UCE, which are discussed below.

Bulk Access to WHOIS data

I cannot conceive of a situation where bulk access to WHOIS data would be required, and as such it should be denied unless required by law. Although there has been some discussion about providing access to Law Enforcement Agencies (LEAs), legal practitioners etc, such requests are likely to be limited to identifying the entity responsible for a given domain. This information is already publicly available and therefore there is no reason to provide for extraordinary access. The security of the database should be vigorously defended by the custodians and where ordered to provide access by courts this access should be restricted where possible (eg. by restricting it to a search for domains registered by a given entity rather than providing a bulk feed).

Restricting Access to WHOIS data

There is currently a query limit of 20 queries per hour on the WHOIS database. I am not convinced that this alone is sufficient to protect the information without inconveniencing legitimate users and I would suggest the security be further enhanced. Some suggestions include:

- Tracking long term query habits
- Quickly blacklisting IPs which have disproportionately high negative returns and who are likely to be brute forcing the database
- Implementing a turing test
- Using cookies to differentiate between users behind a proxy/NAT firewall
- Providing authenticated access with less sensitive tests for power users
- Concealing email addresses (by using web forms and/or generating images of the addresses)

There should also be technical restrictions on registrar interfaces, although these would have to be devised so as not to interfere with their normal operation.

Preventing Domain Name Related UCE

A primary driver for restricting access to WHOIS data is to control domain name related Unsolicited Commercial Email (UCE). This is only one way in which bulk access to WHOIS data can be abused, and it is one which can and should be controlled via other policies. Such policies could invalidate fraudulently solicited transfers and ban offenders from offering domain names, for example. Access to dates has been restricted to tackle exactly this problem and I question as to whether this move was necessary as being able to

determine when a renewal is due or a domain name will be released for re-registration is certainly convenient.

Conclusion

I consider the Australian WHOIS policy to be one of the best in the world. However there is still room for improvement and I would suggest the following changes be made:

- verify information on registration (esp. ABN, ACN)
- re-verify information on renewal
- restrict information available for .id.au domains
- publish relevant dates (esp. expiry)
- improve security by introducing new tests (eg turing test)
- improve usability by modifying existing tests (eg cookies for proxy servers)
- improve usability by authenticating power users/registries/etc.
- identify and block brute force attempts
- modify other policies (eg. to control domain name related UCE)
- document procedures for law enforcement and courts
- continue to provide access to email addresses (but consider obfuscating them by serving images, using web forms, etc.)
- consider the effect of changes on system administrators (eg. removing tech contact info)