

WHOIS POLICY REVIEW, NOVEMBER 2013

Issues Paper

Background

WHOIS is the service that allows people to look up certain details in relation to a registered domain name. WHOIS is a standard feature of the DNS around the world, but the amount of data disclosed on the WHOIS service varies between TLDs.

The WHOIS service discloses only a subset of the data that is held in the registry database. auDA does not currently provide access to other types of registry data, other than to law enforcement bodies.

This review covers the following separate but related questions:

1. Should there be any changes to auDA's WHOIS Policy covering the collection, disclosure and use of WHOIS data for .au domain names?
2. Should access to .au domain name data (other than via WHOIS) be opened up?

auDA held a workshop on WHOIS and data openness at the Australian Internet Governance Forum on 17 October 2013, where many of the issues raised in this paper were discussed by a panel of speakers and audience participants.

1. Should there be any changes to auDA's WHOIS Policy covering the collection, disclosure and use of WHOIS data for .au domain names?

auDA's current [WHOIS Policy \(2010-06\)](#) has been in place since 2010. The data fields that are disclosed on the .au WHOIS service are shown at Schedule A of the policy.

Registrant contact information

Unlike the WHOIS service for .com domain names, the .au WHOIS service does not disclose the registrant's physical address or telephone/facsimile numbers. The only registrant contact information that is disclosed is an email address (which is allowed to be a generic email address – eg. info@domainname.com.au).

It has been argued that, at least in the commercial 2LDs com.au and net.au, more registrant contact information should be disclosed. We note that the ATMOSS database of trade mark registrations discloses a physical address for the trade mark owner (but not an email address), whilst the ASIC database for company and business name registration does not disclose any contact details through the online search tool, but more information can be purchased from ASIC.

Anecdotal evidence suggests that the disclosure of physical address and telephone/facsimile numbers in the .com namespace has resulted in many registrants providing false information, or using privacy and proxy registration services to mask their information. Consequently, the data accuracy and integrity of the .com namespace is widely regarded as very poor. There may be a risk that disclosing more information on the .au WHOIS service will result in the same degradation of accuracy and integrity.

Private or proxy registration services

The WHOIS service discloses the registrant name, registrant ID (where applicable), registrant contact name and a registrant contact email address. auDA policy does not permit a registrant to hide any of these details (although they are permitted to use a

generic contact name and email address – eg. “The Manager” and manager@domainname.com.au).

Anecdotal evidence suggests that many registrants would prefer not to disclose their name and/or contact information on WHOIS. This option exists in other TLDs through various models including:

- WHOIS opt-out services – the registrant’s identity is disclosed, but registrant contact information is removed from WHOIS
- WHOIS privacy services – the registrant’s identity is disclosed, but registrant contact information belongs to the privacy service
- proxy registration services –the registrant’s identity is masked (shown as “Domains by Proxy” or similar) and registrant contact information belongs to the proxy service.

Arguments against allowing use of such services tend to focus on the need for disclosure of registrant identity and/or contact information in the interests of consumer protection, intellectual property rights and law enforcement.

It should be noted, however, that allowing use of WHOIS opt-out or privacy services would merely affect the ability of people to look up registrant information on WHOIS. It would not remove this information from the registry database, and other processes could be implemented to allow access to this information – an example being auDA’s request for creation date process, which has been in place since 2002.

Proxy registration services are in a different category, due to the fact that correct registrant information is not submitted to the registry database and is only known to the provider of the proxy service. It is difficult to see how proxy registration services can be accommodated in a namespace like .au, which requires registrars to verify that registrants meet strict eligibility criteria. One solution may be to restrict the provision of proxy services to accredited registrars, who can verify the correct registrant information and disclose it to auDA on request.

However, consideration also needs to be given to the public interest in knowing that .au registrants comply with the eligibility rules; this is most readily achieved by a member of the public being able to look up a registrant’s details on WHOIS. If this ability was removed, then it may lead to an increase in complaints to registrars and auDA, and a deterioration in the perceived integrity of the namespace.

Domain name creation and expiry dates

auDA removed domain name creation and expiry dates from WHOIS in 2002, in an attempt to prevent the fake renewal notice scams that were causing major problems in the .au market at the time. Removing the dates from WHOIS made it more difficult for scammers to contact a registrant at the time their domain name was due for renewal.

More than ten years later, it may be appropriate to reinstate domain name creation and expiry dates into WHOIS. Disclosing expiry dates would enable registrants to readily check when their domain name is due to be renewed. Disclosing creation dates would assist registrants and other interested parties in tracing the history of a domain name, particularly in cases of ownership dispute or legal rights infringement. It would mean that auDA would no longer have to provide a request process for people who want to know the creation date of a domain name.

auDA invites comments on the issues outlined above, and on any other issues in relation to the current [WHOIS Policy \(2010-06\)](#).

2. Should access to .au domain name data (other than via WHOIS) be opened up?

Currently (and historically) the only public access to .au domain name data is via a WHOIS search. This has a number of limitations, including:

- only allows searching by domain name
- only provides a subset of registrant information
- no bulk access, and the number of look ups allowed per hour is restricted.

auDA does allow access to other types of registry information under protocol arrangements with law enforcement agencies, but only in relation to specified domain names.

auDA also has a process for people to request the creation date of a specified domain name, pursuant to a .au Dispute Resolution Policy (auDRP) or other legal proceeding involving the domain name.

The workshop on 17 October 2013 discussed the following scenarios where people may want access to registry information:

- a. I am a .au registrant – can I search the registry database for a complete list of all my domain names?
- b. I think my details have been used to register .au domain names that have nothing to do with me – can I search the database for a complete list of all domain names using my registrant details, plus any contact details associated with those domains so I can take action?
- c. I am an IP lawyer – can I search the database for a complete list of all domain names belonging to my clients? Or all domain names containing brand names that belong to my clients?
- d. I am an IP lawyer and I think my client's trade mark is being infringed – can I search the database for all domain names containing brand names that belong to my clients, plus any contact details associated with those domains so I can take action?
- e. I am an Australian law enforcement officer conducting an investigation into an Australian person/website – can I search the database for any information that might assist my investigation?

At the workshop, there was general agreement that people should be able to access the registry database for information about themselves and the domain names that they hold. By extension, people should also be able to authorise someone else (eg. a lawyer) to access that information on their behalf.

Workshop attendees were less comfortable with the notion that law enforcement agencies should have open access to the registry database. Privacy concerns were raised, and it was suggested that law enforcement agencies would need to show that their request for information was related to an official investigation or otherwise authorised by a court of competent jurisdiction. It was also suggested that law enforcement requests should be coordinated through a single authorised point and/or a centralised process with auDA.

Some other possible data access scenarios, which were not discussed at the workshop, are:

- g. I am an academic researcher – can I search the database for any information related to my field of inquiry?
- h. I am a commercial marketing data analyst – can I search the database for any information related to my field of inquiry?

There may be other scenarios which should also be considered under this review.

Questions for consideration, which apply to all the above scenarios, include:

- should there be restrictions on the purpose for which registry information can be requested and/or used (eg. only in relation to legal proceedings)?
- should there be a fee for different levels of access to registry information, or for different types of request (eg. commercial versus non-commercial, government versus non-government)?
- what are the privacy implications/rights for .au registrants?

auDA invites comments on the issues outlined above, and on any other issues in relation to data openness in the .au domain.