

Whois Policy Review Submission

From: Ewen McNeill
Received: 4 October 2004

1. Information displayed

I have no particular problem with all the existing information returned by a whois query continuing to be returned, as I believe the information was submitted for, inter alia, the purpose of being displayed as contact information should someone need to reach a person responsible for the domain.

Having said that:

- from an operational point of view the most useful fields are the domain/status/date fields, followed by the nameserver fields, followed by the admin contact email address and contact phone number

- the "technical contact" fields have been abused to the extent that they are being used only for registrar information (once upon a time the technical contact was someone at the organisation the domain belonged to responsible for DNS/technical issues), and I suspect many of the registrar details aren't of much use. The `_name_` of the registrar, their website URL, a contact email address there and perhaps their phone number are the most useful of those details.

(For the avoidance of doubt I believe that the registrar name **MUST** continue to be shown, and that the website URL, contact email address and phone number **SHOULD** continue to be shown; I consider the rest optional.)

- the "admin contact" fields are largely being used in place of what used to be a technical contact. As such as noted above a name of a person, an email address to contact them, and a phone number to contact them are pretty important. These are details that I use routinely when dealing with issues with DNS, and DNS related things (such as email or website issues).

- the postal addresses are nearly useless information from a practical point of view. Its sole benefit in a whois result is in distinguishing between people/organisations with the same name.

(Obviously the SRS still needs to collect this information for contact purposes.) The address details returned in a whois result could probably be safely abbreviated to just name, city, and country with little loss of usefulness. This would have the side benefit of making snail-mail phishing and related scams more difficult.

- as for the fax numbers, does anyone still use faxes? The usefulness of displaying this field seems low, although given it's optional I imagine those who care about its disclosure can simply omit it.

If the approach above (ie, abbreviating address details returned) is adopted, then there is one disadvantage -- nameholders cannot use whois to verify that

the correct details have been submitted to the registry independent of their registrar. I would suggest that a replacement mechanism for this type of verification be provided, perhaps via a page on the DNC website that took a domain name and a UDAI and returned all information held on file. (This would also help to satisfy Privacy Act 1993 considerations.) (To my mind this is a far more legitimate use of the UDAI for authentication than its abuse by various registrars to authenticate non-domain-transfer items.)

As for question 1.4 (difference between information displayed for an individual and an organisation), IMHO there should be no difference, and such a difference is not practically implementable. (What is "an organisation" anyway? A company? An incorporated society? What about unincorporated societies? Partnerships? "Trading As"/"Doing Business As"? Overseas companies? The list goes on.)

2. Whois Query Options

I think the past two years experience has shown that there is no particular need for wildcard whois queries; I have not heard anyone seriously complain about their absence. Google is often a good substitute for the "what domain name do they have" need that was previously served by wildcard whois queries.

Given that a bulk whois query can be used for data mining, and that the legitimate need it once served seems better served in other ways there seems to me no need to enable it.

3. Security and System Access

To some extent the protections against data mining will always rely on "security through obscurity". Providing there is not a significant number of complaints about legitimate whois usage being blocked there is probably no great need to publish details of the exact protections employed. It may, however, be beneficial to publish a summary of some of the more obvious types of protections employed, partly to satisfy registrants that steps are being taken, and partly to satisfy Privacy Act 1993 concerns. (By "obvious types of protections" I mean ones that any reasonably clueful person would have already determined were present.)

I believe that the whois policy should specify the range of actions that the DNC might take to (suspected) whois service abuse, and contain a statement that any actions taken shall be proportionate to the degree of abuse, but I don't think there needs to be a table of "do action X, punishment is Y" -- and I think such a table would be counter productive. (Due to people seeing a "low" punishment and deciding they can afford to try it on.)

General Feedback

The whois service is invaluable for solving day to day operational issues. I strongly oppose any move to take it away. I strongly oppose any moves to make it "web only"; there is a large body of useful existing tools using the standard whois interface (TCP port 43).

I also strongly oppose any moves to put an authentication front end in front of the whois service (as suggested by some) as it will affect only legitimate users (those who are doing "data mining" have a strong incentive to develop automated means around any authentication; those with legitimate uses have neither the time nor the incentive, so would be deprived of a valuable service).

Finally, is there any plan to reinstate the full disclaimer message at the top of the whois queries? The current disclaimer at the top of each whois result is a "one partial sentence" version which was done "so it would be obvious it needed to be corrected before the whois service went live". Apparently not obvious enough, given that we've completed nearly two years without the full version being reinstated.

We also managed nearly two years with the whois server returning the wrong version number (so it didn't correspond to the published specification although only due to the version number conflict), and are now into a period where the whois service does not comply with any published specification for some other reason (it changed about two months ago, but NZRS appears unable to say how -- despite a request, there has no been no update of the Whois server specification forthcoming).

It's been so long I'm not even sure I can find the original wording, but in any event a review of the wording of the disclaimer at the top may be appropriate.