## Q1 Your name (must be a RDS PDP WG Member, not Observer, to participate)

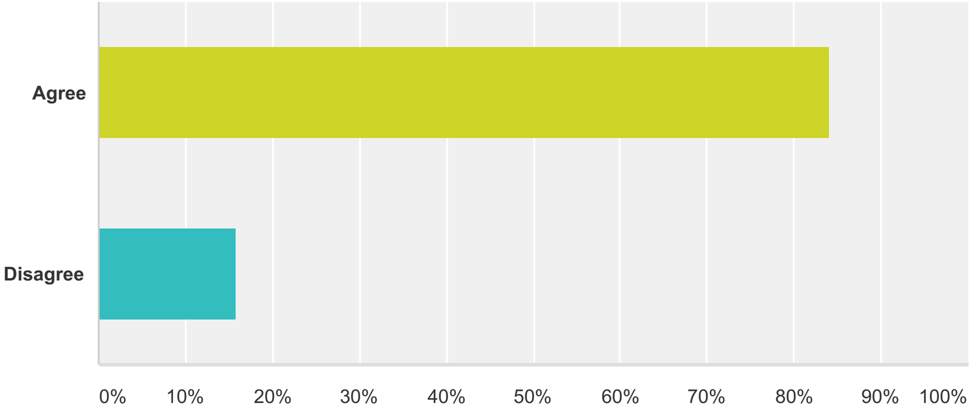
Answered: 38 Skipped: 0

| # | Responses | Date |
|---|---|---|
| 1 | Greg Mounier | 5/7/2017 1:55 AM |
| 2 | Stephanie Perrin | 5/6/2017 5:33 PM |
| 3 | Olevie Kouami | 5/5/2017 11:02 PM |
| 4 | Marc Anderson | 5/5/2017 11:46 AM |
| 5 | Sam Lanfranco | 5/5/2017 10:21 AM |
| 6 | Alex Deacon | 5/5/2017 9:32 AM |
| 7 | Susan Kawaguchi | 5/5/2017 9:26 AM |
| 8 | Ayden Ferdeline | 5/5/2017 9:26 AM |
| 9 | Adam Lanie | 5/5/2017 9:15 AM |
| 10 | Michael Hammer | 5/5/2017 9:10 AM |
| 11 | Rod Rasmussen | 5/4/2017 6:59 PM |
| 12 | Vicky Sheckler | 5/4/2017 11:44 AM |
| 13 | Roger Carney | 5/4/2017 9:21 AM |
| 14 | John Bambenek | 5/4/2017 9:21 AM |
| 15 | Tom Undernehr | 5/4/2017 9:02 AM |
| 16 | Vlad Dinculescu | 5/4/2017 6:36 AM |
| 17 | Juan Manuel Rojas | 5/4/2017 5:21 AM |
| 18 | Tom Lancaster | 5/4/2017 2:23 AM |
| 19 | Cedric Pernet | 5/4/2017 1:26 AM |
| 20 | Farell Folly | 5/3/2017 3:55 PM |
| 21 | Sara Bockey | 5/3/2017 2:07 PM |
| 22 | Alexander Jaeger | 5/3/2017 1:36 PM |
| 23 | Nathalie Coupet | 5/3/2017 10:38 AM |
| 24 | Greg Aaron | 5/3/2017 8:34 AM |
| 25 | Griffin Barnett | 5/3/2017 8:18 AM |
| 26 | Chuck Gomes | 5/3/2017 8:00 AM |
| 27 | Chris Baker | 5/3/2017 7:14 AM |
| 28 | Paul Keating | 5/3/2017 6:30 AM |
| 29 | Scott Hollenbeck | 5/3/2017 5:11 AM |
| 30 | Maxim Alzoba | 5/3/2017 3:19 AM |
| 31 | Klaus Stoll | 5/3/2017 2:20 AM |
| 32 | Patrick Lenihan | 5/2/2017 11:43 PM |
| 33 | David Jevans | 5/2/2017 10:34 PM |
| 34 | Greg Shatan | 5/2/2017 10:27 PM |

| | | |
|---|---|---|
| 35 | allison nixon | 5/2/2017 8:26 PM |
| 36 | Alan Greenberg | 5/2/2017 7:54 PM |
| 37 | Elaine Pruis | 5/2/2017 7:17 PM |
| 38 | Geoffrey Noakes | 5/2/2017 7:14 PM |

## Q2 During deliberation, WG members questioned the meaning of "public" and discussed several different alternative sub-questions. Ultimately, support was expressed by those on the call for the following statement:gTLD registration "thin data" should be accessible without requiring inquirers to identify themselves or state their purpose.Do you agree or disagree with this statement, and why?

Answered: 38 Skipped: 0



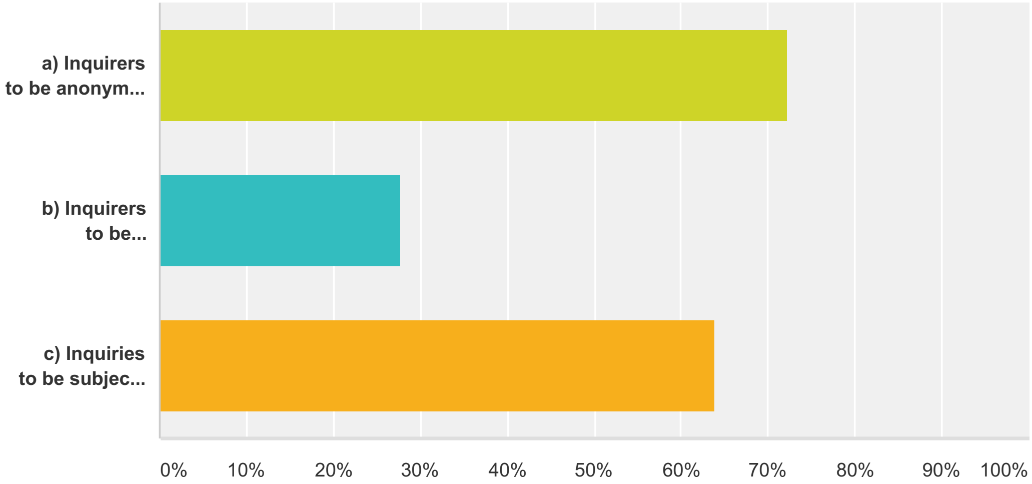
| Answer Choices | Responses | |
|---|---|---|
| Agree | 84.21% | 32 |
| Disagree | 15.79% | 6 |
| Total | | 38 |

| # | Comment Box (for example, give rationale for your answer or suggest an alternative): | Date |
|---|---|---|
| 1 | I am not sure that all the data currently considered "thin" is necessary and I think it should be the minimum. However, in principle I do agree with the statement and concept. I just think we should examine each data element. | 5/6/2017 5:33 PM |
| 2 | I selected disagree on this one. I'm thinking of this in terms of a registrant. As a domain registrant I'm not sure why traditional thin elements such as domain status and dates (registration, expiration and update) MUST be accessible to anyone without requiring inquirers to identify themselves or state their purpose. If as a registrant I had the option (opt in) to publishing this information in the RDS, I would be fine with that. We've heard from several working group members on why having access to the domain date fields is useful in combating abuse. I am supportive of people or companies with that purpose and identified as such being able to access that data (but that's not what is being asked here). As a domain registrant, I don't support all of the traditional thin data elements being accessible without requiring inquirers to identify themselves or state their purpose on a "no opt out" basis. | 5/5/2017 11:46 AM |
| 3 | I would keep it simple and view this as a bilateral or reciprocal relationship in that what has "open access" is "thin data" and "thin data" has "open access". Treat any data with gated access as "thick data" and deal with gated issues there. Let's keep it simple and clean. | 5/5/2017 10:21 AM |
| 4 | This is the minimum information neccessary to verify if a domain is legimate. | 5/5/2017 9:15 AM |
| 5 | Caveat that any such access comes with certain obligations/restrictions - yes, enforcability is an issue, but one still publish terms that if broken, could lead to some sort of action (e.g. harvesting information for DDoS attacks) | 5/4/2017 6:59 PM |

| | | |
|---|---|---|
| 6 | none of the thin data is personally identifiable information and on balance the utility of having the information public for reasons noted on the last call outweigh any potential / presumably unlikely privacy concerns | 5/4/2017 11:44 AM |
| 7 | Thin data is required for troubleshooting and diagnosis. In many cases, the underlying data has to be public (i.e. Authoritative nameservers) or DNS simply will not work. This diagnosis may take place by consumers and end users and expected them to get authority to RDS is probably untenable and gated access to something everyone gets access to makes little sense. | 5/4/2017 9:21 AM |
| 8 | Identifying yourself during an investigation can be dangerous | 5/4/2017 9:02 AM |
| 9 | Because this information is important for anyone who wants to buy a domain could be find when this will be released or since when domain name was taken. This gives more transparency to all process. | 5/4/2017 5:21 AM |
| 10 | Requiring inquirers to identifiy themselves or state their purpose will allow for logging of this information (i.e. who is inquiring about which domains) which is just as much a PII issue as the data that this group is attempting to protect. In addition to this, for other security researchers such as myself, this will add additional paperwork to our everyday work. | 5/4/2017 2:23 AM |
| 11 | purpose needs to be specified | 5/3/2017 3:55 PM |
| 12 | I would agree as this data relates of the domain and its life cycle/function. | 5/3/2017 2:07 PM |
| 13 | There are no PII, nameserver is required for the operation of the Internet; no privacy issues | 5/3/2017 10:38 AM |
| 14 | "Thin" Data elements include technical data sufficient to identify the sponsoring registrar, status of the registration, and creation and expiration dates for each registration in a TLD's WHOIS data store. This data is not personally identifiable information. There is no clear rationale for keeping this information private, and therefore it should be accessible publicly without the need for inquirers to identify themselves or state a purpose in accessing this data. | 5/3/2017 8:18 AM |
| 15 | Open access to data should be the starting point from which limits are implemented to curb abuse | 5/3/2017 7:14 AM |
| 16 | Though I recommend to change the wording to reflect the fact, that implementation of machine readable means of access to RDS data (such as RDAP), will lead to situation where requestors are going to be servers (and not individuals), so I think it could be a good idea to describe the process "without requests for identification of the requestor" rather than " without requiring inquirers themselves" | 5/3/2017 3:19 AM |
| 17 | Basic data should be available regardless of who is inquiring. We need an "open" information system. | 5/2/2017 11:43 PM |
| 18 | yes, the alternative is completely unenforceable anyways, just like whois accuracy is | 5/2/2017 8:26 PM |
| 19 | No privacy issues involved | 5/2/2017 7:14 PM |

## Q3 To help inform next week's deliberation, which if any of the following statements should be further deliberated by the WG as possible requirements for allowing access to "thin data." (check all that apply, if any)Access to gTLD registration "thin data" should allow:

Answered: 36 Skipped: 2



| Answer Choices | Responses | |
|---|---|---|
| a) Inquirers to be anonymous (i.e., access without any identification, as is allowed by today's WHOIS) | **72.22%** | 26 |
| b) Inquirers to be unauthenticated (i.e., require identification, but without any verification of that identity) | **27.78%** | 10 |
| c) Inquiries to be subject to anti-abuse measures such as rate-limiting and CAPTCHA | **63.89%** | 23 |
| **Total Respondents: 36** | | |

| # | Comment Box (for example, give rationale for your answer or suggest an alternative): | Date |
|---|---|---|
| 1 | It is not clear to me what harm would be created by bulk data capture, so I would appreciate further discussion of this. | 5/6/2017 5:33 PM |
| 2 | I am strong on a) & b) as conditions of "thin". I am less strong on c) | 5/5/2017 10:21 AM |
| 3 | a) Access to today's WHOIS does not require identification but I would argue it is not anonymous. (ip address and associated metadata is known) b) Requiring unauthenticated access without verification is pointless. c) anti-abuse measures should be set to a high value - minimizing potential access issues while providing effective anti-abuse properties. | 5/5/2017 9:32 AM |
| 4 | Inquirers MAY be anonymous (and subject to rate-limiting to protect providers) but they MAY choose to authenticate to avoid rate-limiting. | 5/5/2017 9:15 AM |
| 5 | I checked "C" but the devil is always in the details. I believe that an API should be available to individuals and organizations using data for anti-abuse and other existing purposes. For individuals accessing through a web interface I'm not against reasonable (for some definition of reasonable) rate limiting and/or use of CAPTCHA or similar anti-abuse methods. | 5/5/2017 9:10 AM |
| 6 | A) What methods, and is there a way to display terms of access to all? B) What does this accomplish? C) Gaming of these rules to prevent legit access (see current issues with whois!) | 5/4/2017 6:59 PM |

| | | |
|---|---|---|
| 7 | i don't think any should be further deliberated, as there weren't any reasons given for limiting access, other than a "I want to check with my group" response. | 5/4/2017 11:44 AM |
| 8 | I think A and C both make sense. For B, I don't think identification is a requirement, I believe access should be unauthenticated where identification may or may not be provided. | 5/4/2017 9:21 AM |
| 9 | Preventing abuse and scraping is perfectly fine. | 5/4/2017 9:21 AM |
| 10 | We need to keep the ability to pull this information in an automated fashion. | 5/4/2017 9:02 AM |
| 11 | By having all three apply, it keeps the process as it is allowed today while taking steps to reduce abuse. Having requestors ID themselves could be useful, even if voluntary and unverified. | 5/3/2017 2:07 PM |
| 12 | High-limit rate limiting would only prevent very few automated inquiries (special cases such as the case of a company looking up 10K registraant data in a day) and the reward would be anti-abuse protection from web crawler and data harvesting schemes; CAPTCHA would prevent automated searches, which I fear, would result in substantial financial expenses for cybersecurity companies. | 5/3/2017 10:38 AM |
| 13 | Although thin data should remain publicly and anonymously accessible, we have no strong opposition to implementing anti-abuse measures such as rate-limiting or CAPTCHA. | 5/3/2017 8:18 AM |
| 14 | Anti-abuse measures should be an option that registries and registrars may use but should not be required. | 5/3/2017 8:00 AM |
| 15 | Anonymous access should be allowed, however if the cost to the operator of the service is onerous it seems reasonable to implement an authentication mechanism to understand usage patterns. If the unauthenticated access is abused then it is reasonable to use a CAPTCHA or rate-limit to ensure the service is available. | 5/3/2017 7:14 AM |
| 16 | For clarity: I do NOT see that A and B are inconsistent - many current WHOIS sites require Captcha to avoid scraping. I view Captcha and similar to be neutral "restrictions" unrelated to the identification of the requesting party or the purpose of the inquiry. | 5/3/2017 6:30 AM |
| 17 | Option a) could be worded a little differently. Anonymity is not really an available option since the RDDS server will always see the source IP address of the querying client, so I would rephrase a) as "Inquirers to be unidentified (i.e., access without the need to provide identity credentials, as is allowed by today's WHOIS)". Option b) could then be reworded as "Inquirers to be unauthenticated (i.e., require identity credentials, but without any verification of that identity)". | 5/3/2017 5:11 AM |
| 18 | Requiring identification without verification is an exercise in futility. | 5/2/2017 11:43 PM |
| 19 | revoking anonymous whois querying is bad- as a good portion of these types of queries will be for security purposes, and queries against sensitive types of domains (espionage, cyberwar) can result in personal targeting or assassinations. since these logs are of extremely high value in cyberwar, we should accept it as a foregone conclusion that they will be hacked. The concern is large enough that i guarantee my colleagues will explore fake identities and proxy querying. Especially if identity validation is as badly done as it is with whois accuracy. ////////////// the only anti-abuse limiting i would agree with is rate limiting for anti-DDOS purposes only. and this doesn't mean that people can set up on a raspberry pi. it has to be reasonable. i would also be open to a standard agreement existing to have IP addresses whitelisted for mass query volume, to cover the bandwidth costs of the whois server so it is not an undue burden. Also, if bandwidth is a big concern, can any new whois protocol support features like gzip compression? is it possible? | 5/2/2017 8:26 PM |
| 20 | a, b: I already said should not be required. c: must allow bulk automated checking. Perhaps that does not preclude requiring some authorization to do this, but need to hear from people who do this. | 5/2/2017 7:54 PM |
| 21 | It is in the best interest of the Whois provider to pick into place rate limiting and captcha. Since there are no security or stability risks posed by not requiring rate limiting, it should not be a policy requirement but rather optional and at the discretion of the provider. | 5/2/2017 7:17 PM |
| 22 | No privacy issues involved | 5/2/2017 7:14 PM |