This poll closed 21 January with 25 responses, as detailed below.
Related Link: ***PDF of poll questions***

Q1) Confirm **Domain Name Certification** as a purpose for "thin data" collection

Answer Choices	Responses
a) Yes, Domain Name Certification is a legitimate purpose for "thin data" collection.	87.50% 21
b) No, Domain Name Certification is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	12.50% 3
Total	24

Comments (6)

1. I'm not sure that thin data is sufficient for a CA to confirm that a DN is registered to the certificate requestor. I'm also not convinced it's the purpose of RDS to facilitate CAs.

2. DN Certification only becomes a legitimate purpose if such certification is actually undertaken. If no certification is required, it cannot serve as purpose for collection. Collection can occur once certification is requested.

3. While I acknowledge that some CAs use domain registration data and WHOIS services for confirmation purposes, I need to note that it is not the only way to perform this task. The Let's Encrypt initiative, for example, does not use WHOIS - it uses the DNS and publication and verification of content on a web server to demonstrate domain control.

4. The thin data is only part of what the CA needs to issue a certificate to a subject identified by a domain name. I presume that there is some dialogue with the CA's over what thin data best served their needs, as an input into defining the thin data field set. Since the number of CA is finite, might this be an area with some gated access?

5. For this and all other purposes listed herein or otherwise (or no purpose), "thin data" should be publicly available, without any form of gated access.

6. No opinion.

Q2) Confirm **Business Domain Name Purchase or Sale** as a purpose for "thin data" collection

Answer Choices	Responses
a) Yes, Business Domain Name Purchase or Sale is a legitimate purpose for "thin data" collection.	91.30% 21
b) No, Business Domain Name Purchase or Sale is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	8.70% 2
Total	23

Comments (3)

1. What would be the save guards against abuse of this use?
2. This data could also be requested from the seller prior to the purpose.
3. DN sale or purchase should be facilitated by access to thin data, but since the number of sale/purchase agents is large, there should be a minimum set (or subset) of the thin data that specifically addresses this use. That might be as little as expiry date, and a (proxy?) email contact address. More information should be at the discretion of the DN holder, not in the thin data set.

Q3) Confirm **Academic/Public Interest DNS Research** as a purpose for "thin data" collection

Answer Choices	Responses
a) Yes, Academic/Public Interest DNS Research is a legitimate purpose for "thin data" collection.	86.36% 19
b) No, Academic/Public Interest DNS Research is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	13.64% 3
Total	22

Comments (6)

1. Actually, one never collects data solely for the benefit of potential researchers. One allows access. As I have pointed out repeatedly, purpose of collection for all these various applications often conflates (or risks conflating) subsequent use/disclosure for new purposes. . No registrar is collecting data for academia, are they???
2. Yes but it should not be mandatory : and strong justification needs to be given.
3. What would be the save guards against abuse of this use?
4. It would first have to be established what constitutes DNS research and why this data would be needed. It is not a purpose benefiting the domain owner.
5. This purpose effectively justifies curiosity as a reason to obtain thin data. With other purposes I can easily predict what the consumer will need and what will be done with the data. Research in this context is too abstract to provide that kind of understanding.
6. This is both a legitimate and desirable use. There is such a range or academic researchers that gated access would be unmanageable, unless there was a simple process such as an endorsement for access by the researcher's own institution's research ethics process. Non-gated access is data in the public domain and there would be no confidentiality issues with research publication. Their may be confidentiality issues to be dealt with if there is gated access.

Q4) Confirm **Regulatory and Contractual Enforcement** as a purpose for "thin data" collection

Answer Choices	Responses	
a) Yes, Regulatory and Contractual Enforcement is a legitimate purpose for "thin data" collection.	91.67%	22
b) No, Regulatory and Contractual Enforcement is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	8.33%	2
Total		24

Comments (5)

1. Again, data is collected for other purposes. Registrars are not collecting data for tax compliance purposes, they might release data collected for other purposes to investigators, but they do not collect the data for this purpose.
2. What would be the save guards against abuse of this use?
3. Can be a legitimate purpose, but only if there is a legislative requirement for the collection and storage.
4. It isnt clear why the tax office needs to know the name servers or last updated date. Why does the Tax office need to know the Registration status or the sponsor? UDRP and URS are supposed to apply at the moment in time they commence (hence why they request locks at commencement), so last updated seems irrelevant. Should we have "thinner" data elements, list each element with specific needs in each case or simply go with the standard thin data because it is the path of least resistance from a technical delivery point of view?
5. Yes, but this looks like a rich area for lawyers and authorities to design appropriate request and access procedures.

Q5) Confirm **Criminal Investigation & DNS Abuse Mitigation** as a purpose for "thin data" collection

Answer Choices	Responses	
a) Yes,Criminal Investigation & DNS Abuse Mitigation is a legitimate purpose for "thin data" collection.	95.83%	23
b) No, Criminal Investigation & DNS Abuse Mitigation is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	4.17%	1
Total		24

Comments (3)

1. Once again, no data elements ought to be collected for the purposes of criminal investigation. They might be released to investigators for the purpose of detecting and prosecuting crime related to a website or electronic commerce activity associated with a domain name, but it is not the purpose of collection.
2. What would be the save guards against abuse of this use?
3. There are two issues here. Along with everybody else LEAs would have access to non-gated data. For gated access what would constitute adequate legal authority? Access would be to what (all or some) data?

Q6) Confirm **Legal Actions** as a purpose for "thin data" collection

Answer Choices	Responses
a) Yes, Legal Actions is a legitimate purpose for "thin data" collection.	88.00% 22
b) No, Legal Actions is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	12.00% 3
Total	25

Comments (4)

1. No, data is not collected for this purpose, it is released for this purpose. Data elements may be collected for the purpose of establishing the parameters of a legitimate registration of a domain name (ie who is the beneficial registrant etc). It is not collected for the purposes of facilitating legal actions.
2. Other areas that may potentially trigger such action do not require the collection of similar data.
3. there are no data elements listed. Am I agreeing to legitimate use of all thin data elements, some or just the domain name? -which seems a little pointless
4. This is a blend of the purposes on Q2, Q4, and Q5 so the task of developing appropriate procedures to authorize access, and for access to what, are essential here.

Q7) Confirm **Individual Internet Use** as a purpose for "thin data" collection

Answer Choices	Responses
a) Yes, Individual Internet Use is a legitimate purpose for "thin data" collection.	95.65% 22
b) No, Individual Internet Use is NOT a legitimate purpose for "thin data" collection. (Please provide rationale in the comment box below.)	4.35% 1
Total	23

Comments (4)

1. IN this case, the thin data collected actually is collected for the limited purpose of contact, so I agree. Note the difference in wording between this question, and the previous one.
2. It can be a source for data collection for non legitime purpose as anyone can therefore collect anybody else data.
3. I know I personally wouldnt read whois output and then expect a warm trusting glow to fill me, but there's no harm in allowing people to view it. As with other purposes, thin data elements are not explicitly listed in the above text.
4. Individuals should be treated in the same way as business interests here (see Q2). When that access is not enough, and the issue is serious enough, the individual can resort to the legal options for greater access

Q8) In our 24 January call, we will discuss the possibility of publishing raw poll data, taking into consideration WG member wishes for privacy and transparency. As input to that discussion, please identify any personal data that you would prefer NOT to be included in raw data that might be published for future WG polls. (Check all data of concern to you, if any)

Answer Choices	Responses
a) WG Member Name	34.78% 8
b) IP Address of the device used to submit poll responses	82.61% 19
c) PDF of your individual poll responses, with or without your name and/or IP address	39.13% 9
d) Other Data (please describe below) Responses	30.43% 7
Total Respondents: 23	

Write-in Responses for choice d)

1. IP data would not be useful or insightful. Many WG members work in a variety of locations, offices, airports, coffee shops. For instance, I completed this poll while WFH on a Comcast IP. This would not be useful identifying data.

2. Do not check the box automatically when I put the comment in. There is no purpose that I can see in collecting or disclosing the IP address, I suggest you dump them.

3. Just responding to b above - I don't think publishing the IP address is actually helpful or would add to the transparency of the poll. Subbing IP for name isn't a great idea and is easily gamed or confusing to others. Plus if the idea is to obfuscate names, but it's obvious based on the IP who the person is (company name, unique country) then you've provided a way to tease out some responders but not others.

4. Device type, location, time, etc. Working group members should feel no pressure, from affiliation or otherwise, in answering questions and PII gives leverage for pressure.

5. You may disclose any information I contribute, share, express etc with any ICANN group.

6. All were ticked NO, for the moment, because this requires further thought. Less privacy may result in poorer responses, and greater transparency may not serve meaningful purposes.

7. Not sure why IP Address is needed, unless it is a proxy for member name. If name is not being given, I'm fine with IP address. Member affiliation should also be listed, I think (with the caveat that a member may not be speaking for the group).