21 Dec Call – Poll on Purpose – Final Results as of 7 January

This poll closed at COB January 7, 2017 with 34 responses, detailed below.
Related Link: *PDF of poll questions*

Q1 (Confirm continued deliberation on purpose of thin data)

Answer Choices	Responses	
a) Yes, the WG should continue deliberation on the purpose of "thin data."	88.24%	30
b) No, the WG should not consider the purpose of "thin data" at all.	11.76%	4
Total		34

Comments (14)

Comment Box	
1.	Continuing references to "the purpose" remain confusing, as noted below there may be multiple purposes. Also note the question in text does not line up with the answers provided.
2.	To be clear "thin data" as defined (extrapolated from the definition of "thin registry") by the Thick WHOIS encompasses the following data elements: domain name, Registrar IANA ID, EPP Status(es), create date, expiration date, update date, name server(s), URL of Registrar WHOIS service. I think it is a great idea to work from this small subset of registration data and once complete move on and iterate with the "next" proposed element.
3.	Linking purpose to thin data is essential. Without purpose one cannot justify why a certain piece of data is being collected. I think it is crucial that we deliberate and find the purpose for each piece of thin data so that the end result proves the rationale and thought process of the working group.
4.	Thin data accords to the principle of data limitation. This is a fundamental of data protection. Also accords to basic info security. Deliberation on what the bare minimum necessary for functionality is, is worthwhile in my view.
5.	I'm uncomfortable with (b) because it suggests closing the avenue. I think that _for now_ it would be useful to say, "Let's just accept the thin data case as a bloc for the sake of argument, and see whether we can make other progress." That doesn't mean I think every data element of the "thin data" group falls into the same category. Compared to the registrant's home address, however, it seems a no-brainer.
6.	I feel like focusing the conversation on "thin data" has unnecessarily boxed the thinking of the PDP into outdated Whois concepts.
7.	The thick whois model is a non-sustainable system future wise. With increasing changes when it comes to privacy laws and an unstable political landscape the thin whois model seems to be the right solution. That being said, a boatload of policies will require change but from a technical point of view this is peanuts compared to the challenges that are ahead of us.
8.	I was swayed by the observation that certain privacy regulations (the EU in particular) require that all information about people be limited by purpose. While the "thin data" is not always personally identifiable, I can imagine that in some cases it is and it can be correlated with other data to become personally identifiable. It seems like we must define some legitimate purpose for "thin data". I do NOT think that we need to define any illegitimate purposes for this data.
9.	Without discussion on the purpose the who discussion has no basis.
10.	No purpose should ever be necessary at all to view thin data, so continuing to deliberate on it implies that some purposes are legitimate and some are not.
11.	I think that progress here rests on two decisions to be made. Consensus on how "thin" (which fields) a "thin data" set should be, based on a soft list of legitimate uses (i.e., reasonable general uses). What is the gain from addressing "illegitimate purposes" in any depth beyond saying something like "illegal uses will be dealt with by the appropriate legal authorities", and listing the obvious (e.g., harvesting data, which won't get far with thin data) That should be enough. There is no reason for ICANN to try to list what constitutes illegal uses, which may actually vary by jurisdiction.
12.	While we should look at "thin data" as a category or slice of data to be managed, that does not mean that there should be any limitations on public display and availability of thin data, including limitations based on purpose. I'm also concerned that after years of moving toward Thick Whois, a re-emphasis on thin data could lead us backwards. Among other things, "thin data" as defined here includes " the URL for the registrar's Whois service." While this is historically accurate for legacy gTLDs, this should be handled with care looking forward, as this item assumes that a "thick" approach will not be adopted. This is an inappropriate assumption, even inadvertently.
13.	The deliberation doesn't provide any new thoughts or suggestions for something better, only showing there are lack of understanding for what these data are used for in the real world and by users not familiar with the reasoning behind why they are there.
14.	We are looking at a complete overhaul of registration data, so anything should be on the table.

Q2 (confirm requirement that every thin data element have at least one purpose)

Answer Choices	Responses	
a) Yes, every "thin data" element should have at least one legitimate purpose.	93.75%	30
b) No, the WG should not require there be legitimate purpose(s) for each "thin data" element.	6.25%	2
Total		32

Comments (13)

Comment Box	
1.	I completely agree there should be a purpose for each element, though I thought we already agreed that this was the case for any registration data element, not just thin data?
2.	Completely agree.
3.	Just to note that we have not really decided what a legitimate purpose is...but the circularity of our thought processes does not preclude this approach.
4.	I'm not comfortable agreeing with either of these statements. My take away was that a legitimate purpose could be found for almost anything and that "requiring" a legitimate purpose for each data element is unenforceable. This does not seem like a direction the PDP should focus on.
5.	If these data elements contain personal data, then yes. With the new EU GDPR and increasing privacy laws, we should use privacy by design. If we do not adopt that into our discussions, then the RDS will face severe implementation issues. We develop software as there is an idea. But if the idea is in conflict with the EU GDPR then we stop developing it until we solve those issues first. The far-reaching consequences of not using privacy by design will make or break a company.
6.	We need to be careful in how we are defining "legitimate", but other than that I agree.
7.	Again, why have thin data if it has no purpose.
8.	I assume we are talking about the existing fields within thin data? (As opposed to changing what is currently defined as "thin data.") If so, no, there shouldn't be a requirement for a legitimate purpose -- this is simply too intrusive.
9.	I checked "NO" but basically want to convey the position that the "think data" should provide a basic set of data as a starting point for general information about a particular domain name. It is the fields both individually and all together that should serve legitimate purposes (one is enough).
10.	Since there are multiple legitimate purposes for each thin data element, this question has no effect, as a practical matter. However, as a philosophical matter, I am answering no, because "purpose" should not be turned into an all-powerful tool that drives every other decision in this WG
11.	Both yes and no, Yes there are obvious legitimate purpose on each of them and therefore that task should be easily accomplished No because it should be obvious, so to demand it to have a legitimate purpose are kind of stating the obvious.
12.	Just want to clarify, while I am generally supportive of all RDS elements having a legitimate purpose that are mandated by ICANN, I believe individuals registries should be able to self determine which additional data elements they may choose to add for their legitimate business purposes.
13.	If there is no purpose for provision or storage of such data, there is also no need.

Q3 (confirm every existing thin data element has at least one legit purpose for collection)

Answer Choices	Responses	
a) Yes, there is at least one legitimate purpose for collecting all of these "thin data" elements.	90.91%	30
b) No, there is no legitimate purpose for collecting one or more of these "thin data" elements. (If you disagree, please explain why in the comment box below and identify any "thin data" elements for which you do not think there is a legitimate purpose for collecting the data.)	9.09%	3
Total		33

Comments (8)

Comment Box	
1.	Although I do agree with the statement, I am still very much on the fence about some of the elements and their purpose. I would like to see the WG members who provided purposes for some elements provide the WG with some real-life examples and processes for use of the data. For example, I understand that the Last Updated field shows when the domain name was last updated, and that the purpose of this element is to identify when the last change was made, for legal proceedings. But from my view it does not tell me what was updated, by who, and to what. I'm seeing the process going back to the registry for more information, therefore why have the field? A real-world example would be very beneficial to help me see a more concrete purpose behind this field.
2.	Not to quibble, but the entity collecting the data (or generating it) is the registrar/registry or their subcontracted resellers and actors. Not the RDS (which is still a mythical beast at the moment). Placing data in the RDS is an act of display, or sharing, because by definition more actors have access to it. Public display is another matter entirely.
3.	I also think that here is at least one legitimate purpose for PUBLISHING (making available in an RDS) all of the "thin data" elements.
4.	It's difficult to say that any data element doesn't have at least one legitimate purpose. As stated above you can find a purpose for almost anything. That's a bad bar to use. I also think its difficult to decide if a data element is necessary when the PDP hasn't agreed on a RDS purpose. While there are plenty of purposes for "Registrar IANA ID", "Whois Server" and "Referral URL", I don't think those fields are needed. I also think the focus of this question on "collection" of data is problematic. Collection by who? Are we focused solely on the collection of registration data by the registry?
5.	Access to data must have a legitimate purpose that is the currently the case for the current EU GDPR and will continue. And currently displaying personal info is in violation of the EU GDPR.
6.	The collection of (or more specifically the generation/creation of) those items being described as 'thin-data' elements is a necessary function in the role of Registries and Registrars. Whether that needs to be "further collected" (into an RDS) is something I'm not completely sure of
7.	This is worded confusingly, but I think I'm agreeing that for every thin data element, there exists at least one plausible reason for collecting it. True. But, again, we shouldn't be judging who has a legitimate purpose and who doesn't.
8.	Pretty much stated rationale in Q1 & Q2

Q4 (confirm agreement with EWG-identified purposes as they apply to thin data collection)

Answer Choices	Responses	
a) Yes, each of the EWG-identified purposes listed above apply to at least one "thin data" element.	91.18%	31
b) No, at least one of the above-listed purposes do not apply to any "thin data" element. (If you disagree, please explain why in the comment box below and identify any listed purpose(s) that you do not see as legitimate for "thin data" elements.)	8.82%	3
Total		34

Comments (7)

Comment Box	
1.	I do agree that you can apply all 7 of these purposes to one or more of the "thin data" elements but I would question if all of the listed purposes/tasks are valid purposes that the ICANN RDS must account for.
2.	The fact that the purposes listed above apply to at least one thin data element does not mean they apply to all the data elements. I am concerned, as I was when the EWG drafted these purposes, that isolated instances of permissible disclosure are being used to justify wholesale collection and display.
3.	Domain Name Control can be done strictly based on a registrant/registrar basis, with no need for WHOIS/RDS. A possible exception is the creation of the DN itself, and the use case where a registrant loses information about which registrar they are using (easily possible for companies, or indeed people with person administration as chaotic as my own). Also note that the "thin data" on its own does not provide a full solution to most of these purposes. That's okay, as long as it is well understood. :)
4.	...until someone can demonstrate that one of the issues does not relate.
5.	there are multiple mentions of *registrant* and *contact information* which are not thin-data elements
6.	Yes. These are only partial lists, by the way, so other reasons may exist, but I think those are correct.
7.	I don't disagree, but I do think UDRP and URS investigation is misclassified, as it is put under "Regulatory and Contractual Enforcement." But since this is a prior source, that's not really important at this point.

Q5 (Describe any alternative purposes or rationale for why there are no purposes for thin data)

1.	The list provided by EWG is not exhaustive, in my view. For instance, abuse investigations are not necessarily "criminal" and there are other legitimate investigative purposes. i
2.	As mentioned earlier, I would like more in-depth explanations and real-world examples of the purpose of the thin data.
3.	As discussed above, the data has already been collected/generated. What we are talking about here is disclosure. IF we wish to talk about the RDS as an entity, capable of collection, use and disclosure, then we need to define exactly what it is, who is accountable etc. We are talking about a proposed data display mechanism as if it were an entity. If indeed it is such an entity, I am afraid I do not understand its agency.
4.	This survey seems to suggest a course where RDS should collect every data element that has an identifiable legitimate purpose. That casts to wide of a net and makes it very difficult to keep any data elements out of RDS.
5.	Intellectual property rights enforcement could be an alternative legitimate purpose for collecting certain thin data, such as domain status and creation/expiration dates.
6.	Consumer protection and risk mitigation is a legitimate purpose. My company assists banks and payment providers in assessing merchant risk, and also assists consumers. There are a variety of ways in which we access all fields in the Whois record (thin and thick) to measure and predict risk to consumers -- various fields are weighted differently but every one is relevant. So, consumer protection in the payments, consumer and financial space.
7.	I have no suggested alternative purposes but would step back and ask whether or not any particular stakeholder with a legitimate public right to access is being denied some obviously important. This obviously does not address LEA access by legal means, which is a separate issue.
8.	Consumer Trust and Verification -- while thin data is not nearly as useful as thick data in helping consumers verify that a site is legitimate, it's a start, especially if it provides a link to the "thick" elements (which, as noted above, should not be presumed to be on each registrar's WHOIS server).
9.	I would request more information to be provided on the DNS Servers. If a DNS is listed - should it be listed for public view? What is the relevance of listing the DNS?