ICANN Transcription
GNSO Next-Gen RDS PDP Working Group
Tuesday, 6 June 2017 16:00 1600 UTC

Note: The following is the output of transcribing from an audio recording of GNSO Next-Gen RDS PDP Working Group call on the Tuesday, 06 June 2017 at 16:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance may be found at:
https://community.icann.org/x/IsPRAw
The audio is also available at:
https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-06jun17-en.mp3 AND
https://participate.icann.org/p6sxtd7tffa/

Coordinator: The recordings have started, you may now proceed.

Michelle DeSmyter: Great, thank you so much. Well good morning, good afternoon and good evening to all. Welcome to the GNSO Next Gen RDS PDP Working Group call on the 6th of June, 2017 at 1600 UTC. In the interest of time there will be no roll call as we have quite a few participants online, attendance will be taken via the Adobe Connect room so if you are only on the audio bridge could you please let yourself be known now?

All right hearing no names, I would also like to remind all participants to please state your name before speaking for transcription purposes and please keep your phone sent microphones on mute when not speaking to avoid any background noise. With this I will hand the meeting back over to Chuck Gomes.

Chuck Gomes: Thanks, Michelle. And thanks everyone for joining us today. Let me start off by asking if anyone has an update to a statement of interest, please raise

your hands in Adobe if you do. Assuming we don't have anybody that's not in Adobe since nobody identified themselves. Not seeing any hands, let's move right on to the next item in the agenda, which is completing the deliberation on what steps should be taken to control thin data access. And let's take a look at the poll results. Hopefully many of you had a chance to do that already. And we will start with Question 2.

And noting that 24 people responded to the poll. So on Question 2, pretty clear results of there. The statement was at least a defined set of thin data elements and must be accessible by unauthenticated RDS users. The leadership team decided that we can just declare this as a tentative conclusion that will lead toward document.

Daniel Nanghaka: Daniel on the phone bridge for the moment.

((Crosstalk))

Chuck Gomes: Is that you, Daniel?

Daniel Nanghaka: Yes, it's me, Daniel. I'll be connecting to the AC later on in a couple of probably 15-20 minutes.

Chuck Gomes: Thank you. And in the meantime you know what to do.

((Crosstalk))

Chuck Gomes: Okay, right so we had over 90% agree with that. We did review the comments that we are not going to take any time on this call to discuss the comments unless somebody particularly wants to by raising your hand, and so we will move right on to Question Number 2 - or excuse me, Question Number 3, the second question of substance, okay.

Question Number 3, the statement was, RDS policy must state purposes for public access to thin data, 75% of those who responded agreed. We had six people who disagreed. And had some interesting comments. And mainly what I'm going to do is just comment on some of the comments. One of the persistent comments in all of them, there was a least six people that said - excuse me, I'm jumping ahead.

There were three comments I think that I'll comment on. Number 1, and you have scrolling capability so you're able to scroll down to the comments for Question 3, which I think they start on the bottom of Page 4 and end on Page 5 for those of you looking at Adobe there. The first comment and the sixth comment say that it's impossible to predetermine all legitimate uses. Totally agree, it is. And nobody is claiming that it is, okay.

The - nor do I think that this particular statement says that we have to identify. Obviously it's probably in the community's best interest if we identify as many as we can. But there will probably be new ones that come up over time and so forth, so just that brief comment there.

And then on Comment 6, the question is asked, what's the point of stating such requirements if you can't verify or enforce them? Well, part of it is part of our charter in identifying purposes, and another thing is - and we are still analyzing laws from some jurisdictions and so forth but certainly we've seen some requirements in some jurisdictions that require that so that's a couple reasons why we are stating those.

And Comment 7, it says the thin data should not be gated in any way, there is nothing in the statement that says thin data should be gated. In fact I think we've said - we are saying just the opposite so I suspect that's understood. Greg Shatan, your hand's up. Go ahead.

Greg Shatan: Thank you. It's Greg Shatan for the record. And I apologize for not having participated in the poll but if I had then six would have been seven in terms of

disagreement. Purpose is a thread which when pulled under certain laws in certain directions can serve as a gate. That's the problem here. You know, we've cut the questions up so finely that we're not able to actually see the effect of the answers to those questions. Thin data arguably at least is not covered by those laws that require purpose for access. And there are of course a lot of different laws so we are not dealing with any statement about the laws is going to be by definition oversimplified, including any statement I make.

But, if purposes required for access and if purpose has to be predetermined in order for informed consent to be given, then the idea of open ended idea of a non-exhaustive list of legitimate purposes is at odds with the idea that informed consent can't add new purposes unless you go back and get new content from everyone.

So, you know, we are still somewhat floundering with a lack of objective legal advice. And of trying to find a way through all this, but the point is that purpose is not an innocent question when applied by certain people under certain laws in terms of assuring freedom of access to thin data. To my mind that's our ultimate goal is freedom of access to thin data. And there are ways in which answering what seem to be innocuous questions about purpose are directly opposed to that goal. Thank you.

Chuck Gomes: Thanks, Greg. Just two quick responses. We're certainly not using purpose as a gate for anyone who wants access. Certainly we're not recommending that. And secondly, we have talked nothing about consent nor does this statement have anything to do with someone giving consent. Michael, go ahead.

Michael Hammer: Michael Hammer for the record. So on one level I agree with Greg, but I also think based on what he's saying and some of the comments and some previous discussion people are kind of conflating the purpose of the individual who's accessing thin data and the purpose of making it available, right? So

quite honestly, I think we can't control or read the minds of whoever's asking to - or accessing thin data. But this group has certain purposes in making saying data should be available - thin data should be available and that's really the important purpose that should be stated.

And it can be stated in broad measure if you will. We don't have to enumerate every single potential purpose that individuals might have; we can enumerate broad reasons as to why it's important this should be available. All I got.

Chuck Gomes: Thanks, Michael. And note, and I think this is consistent with what you just said, this says RDS policy must state purposes. Doesn't say the requester has to state a purpose so that's important. Okay. Any other comments on this?

The leadership team, again, thought that - we don't have a strong as agreement on this but 3/4 isn't bad and we didn't think that the comments were persuasive enough to spend a lot of time on this one. And so our recommendation is to treat is as a rough consensus conclusion at this point in time. As always with our tentative conclusions, we can revisit them later. Greg, go ahead.

Greg Shatan: It's Greg Shatan again for the record. Just to briefly reply, I think this again goes back to the issue of slicing the question so thin that we're not seeing the - we're losing the forest for the tree. I agree that we need to discuss purpose and understand it. I think what we need to avoid falling into the trap of is defining purpose for collection in a way that it then limits purpose of access. And my understanding is that not necessarily with regard to thin data, but with regard to PII, personally identifiable information, that at least the expressing the purpose for which it might be disseminated later, has to be communicated at the time that the data is collected and consent for any dissemination of the data is secured.

So there may be some conflation involved. And I may be guilty of that. But the purpose is just - it's not only an innocuous concept; obviously we're not - things can't be done purposelessly but we need to watch out for purpose being used in the form of a gate further on down. Thank you.

Chuck Gomes: Thanks, Greg. Jonathan, your turn.

Jonathan Matkowsky: Hi, Jonathan here. I think the point you made is an excellent one that - and that is that the user doesn't have to state the purpose but that the data is being provided based on a purpose. And I think that the language could be clarified to avoid that ambiguity which I think - I tried to really express in the comment although I think it's really beside the point. The main point is that the data elements must be accessed based on - must be provided, right, based on certain - for certain purposes. But that's very different than saying that they must be based on a stated purpose which implies that the user must state the purpose to access it, like Greg was saying.

So if we can clarify that I think it would put a lot of the concerns - I don't want to speak for Greg, but it would - I have the same concern that he was raising. And it would put that concern to bed.

Chuck Gomes: Jonathan, how would you clarify that?

Jonathan Matkowsky: There's probably a few ways. One way would be to determine misuse and promote accountability, data elements - all data elements must be provided based on - for certain purposes.

Chuck Gomes: So, you know, one of the things that takes enormous amounts of time in this working group is when we start word smithing. And there are times when word smithing needs to be done, but I think there are a lot of times when we can spend our time a lot better on other things, on bigger issues than word smithing.

But let's listen to Jim Galvin, see what he has to say.

Jim Galvin: So thank you Chuck. I guess I have a question and I'm not sure if you want to defer this answer, that's fine, sort of looking in the chat room here too, I mean, I have in my own mind and my question is whether or not this aligns - whether folks are thinking or not about a very simple purpose for thin data. It is intended to be something which is generally available and unrestricted, and I'm thinking in terms of, you know, we need to state a purpose that aligns with that and I've always been feeling that we need thin data for the proper operation of the Internet and for the proper, you know, beginnings of dealing - of having anything to do with abuse services.

And I'm thinking that eventually we're going to get around to stating that, that there's a very specific technical purpose for thin data, and it just means it's generally applicable and part of the purpose statement will be that it has to be generally available. Now I don't know, maybe that's going too far for this discussion. Lisa was sort of on the right track there when she's saying our proposed agreement at the moment is that we need a stated purpose.

But I'm imagining a very broad kind of purpose which makes this data generally available and matches where we are. And I don't know, I hope that's helpful. Thanks, Chuck.

Chuck Gomes: Thanks, Jim. Chuck speaking. And we're actually hoping in this agenda today to talk about purposes of even specific thin data elements based on information that's been in this working group as well as the EWG. So now Lisa, were you - in your wording there, bear with me a second, notice that…

Lisa Phifer: Chuck, I was just noting…

((Crosstalk))

Lisa Phifer: I'm sorry, this is Lisa Phifer for the record. I was just noting that when Jonathan started to suggest alternative phrasing, he was actually rephrasing the original EWG principle and had missed the actual working group agreement that was discussed last week…

((Crosstalk))

Chuck Gomes: Okay. Thanks. Okay. Anyone else want to comment?

Jim Galvin: You could see my comments in the chat.

Chuck Gomes: Okay. All right, I'm going to suggest we go ahead and accept this one as a tentative conclusion and I'm sure there are plenty of people, including those who spoke, who will make sure that we don't misuse that principle going forward as we get into thick data and talk more specifically about access to thick data.

All right, Question 4, if you want to scroll down in Adobe or if you have it elsewhere. The statement that was put in Question 4, "Was RDS policies for access to thin data must be nondiscriminatory for all legitimate purposes." Now on this one, there were six commenters who expressed concern about the term "legitimate purposes." Okay. So I want to call attention to that. Obviously that's an important concern.

And so I'll let you identify those - I mean, you can see those. Comment 1 didn't directly mention legitimate services, although I think there's a connection. You can see Comment 2, 5, 7, 8, 9 and 11 all express concern about the term "legitimate purposes." So clearly - and this - we didn't spend enough time on this one last week to actually say that there was pretty good agreement on the call so this one we should spend a little more time on.

One of the things that could be done to this based on the concerns about legitimate purposes would be just to delete that clause at the end and just

say, “RDS policies for access to thin data must be nondiscriminatory.” So I’ll throw that out for discussion. And, Lisa, go ahead.

Lisa Phifer: Sorry, Chuck. That was an old hand. But I will point out that we actually did have some proposed alternative text to throw out there, which I’ll put in chat which tried to explain a little bit better what nondiscriminatory might be.

Chuck Gomes: Thank you. Okay so we’re all watching the chat. And one of the concerns people had was that nondiscriminatory needs to be defined .and actually we did, in the leadership call yesterday, discuss a fairly simple and I think reasonable definition of nondiscriminatory that Lisa will put in the chat. So in the meantime, Jim, go ahead.

Jim Galvin: Thanks, Chuck. Jim Galvin for the record. I just want to highlight, you know, one of the comments down there in particular because I do, you know, rather agree with this just from a logical point of view, you know, comment Number 4, I mean, I don't think this particular question adds anything nor does it really take anything away from what we're doing, you know, given agreement on the previous question.

I mean, given that you’ve got non - or unauthenticated access to the data, it just really does not even follow logically to suggest that it’s got to be nondiscriminatory because what else could you do? You just have got nothing to work with to do anything different. So I guess I’m struggling to understand you know, I don't even know why we have this - this question just doesn’t seem to be - give us any additional information or clarity once we have agreement on the previous one. Thank you.

Chuck Gomes: Thanks, Jim. That seems like a valid point. I guess you would say we don't even need this principle, is that right?

Jim Galvin: That’s correct, thank you.

Chuck Gomes: Okay. How many in the - let's just do a quick Adobe poll, how many of you would like to see this principle remain in there, put a green check. Or if you think it's unnecessary just put a red X. and while you're putting your marks in Adobe, go ahead, Andrew, oh no, I'm sorry, that's just a red X, I'm sorry, I thought it was a hand before. Jonathan, you have your hand up. Go ahead and speak.

Jonathan Matkowsky: So I guess the question we're trying to get at is how could you have discriminatory access if there's no authentication. But I suppose wouldn't that be for like blind people for example, if they can access Whois that would be discriminatory and nonauthenticated?

Chuck Gomes: So I think you're saying the same thing Jim did, if I understand you correctly, is that it's probably - it may not be needed, okay?

Jonathan Matkowsky: Well, I would say that the idea that it be - access be nondiscriminatory may very well be needed even though the rest of it could go. And I suppose that's what I'll say.

Chuck Gomes: Say that for me again, I didn't quite get it, Jonathan.

Jonathan Matkowsky: I could be wrong too. But the way I read this, we were sort of asking, well, if it's nondiscriminatory then maybe the whole thing can go because it's - we're not going to have authenticated access anyway. So if we all agree that the legitimate purposes can go then why do we even need the principle that it's nondiscriminatory to begin with?

And I was just wondering aloud if that's - whether the example I gave as someone who's blind should be able to access Whois, that would be an example where we do need the principle that it be nondiscriminatory even though it's unauthenticated and therefore we wouldn't need, you know, all legitimate purposes to be included, but that access be nondiscriminatory would have a meaning, it would add some purpose like in the example I gave.

Chuck Gomes: Okay thank you - thanks, Jonathan. Now please leave your red Xs and green checkmarks in there and I'd appreciate it if others would express an opinion if you have one. Let's go to Jim Galvin.

Jim Galvin: So, Chuck, I'll go but I wanted to defer to Andrew. He has both the red X and his hand up. It's just poorly displayed there.

Chuck Gomes: Oh, I can't see the hand…

((Crosstalk))

Jim Galvin: If you want to go to Andrew first?

Chuck Gomes: Yes, Andrew, please go ahead.

Andrew Sullivan: Oh, I didn't intend to put my hand up, it was an accident.

Chuck Gomes: Okay. Thanks. I didn't see it anymore, so thanks, Andrew. Okay, Jonathan is that a new hand?

Jim Galvin: Okay so then I'll…

((Crosstalk))

Jim Galvin: Yes, I did actually want to comment and thank you. In responding to the nondiscriminatory discussion that Jonathan was raising, I mean, while I agree that Jonathan raises a valid point in terms of wanting to deal with nondiscriminatory access, I think that that's a user interface issue and that's a whole separate policy discussion that I don't think is, in my opinion, would not be in scope for this particular discussion. But I do think he makes a point that we should not lose track of and we should latch onto.

And then, you know, Bill makes a comment - Bill Fanelli - makes a comment in the chat room about, you know, operational concerns. And I agree too that, you know, I want to categorize the kinds of things that Bill's talking about there as an operational issue and I think that's also separate from this discussion and not really in scope for here. And I don't, at least personally don't include that in the definition of nondiscriminatory. Thank you.

Chuck Gomes: Thanks, Jim. And as a lot of you know, especially those that were on the call last week, we kind of got into some of this. And we were not really focusing on that kind of discrimination that happens on the operational level all the time. So but Bill does make a good point. So and I'm just looking - let me while I try and catch up in the chat a little bit, let me go to Greg and then we'll go to Lisa.

Greg Shatan: Thanks. Greg Shatan. I think part of the problem here is we don't quite know what we mean by nondiscriminatory. Jonathan points out a use that is essentially a human rights or civil rights type of discrimination against a particular type of user. And I agree that's a user interface issue, and I actually practice Web accessibility law so if we wanted to get that point I can be helpful on that. But it is not something that falls into a requirement for the database itself or even, you know, rules of access.

And, you know, other uses here have to do with avoiding essentially perhaps illegitimate access such as bots. When I saw nondiscriminatory my thoughts, you know, went straight to kind of net neutrality type of uses of the term nondiscriminatory. But unless we know why we're putting this rule in here, trying to find a justification for it is to my mind kind of six characters in search of an author or six blind men and an elephant. We don't need to justify having the statement. Rather, we have to figure out what practical purpose we need requires this statement and if we can't find one then I agree with Andrew that we don't have it.

But of course if we do in fact have something that we can consider nondiscriminatory access or a discrimination problem that needs to be solved and also making sure that there aren't good reasons for discrimination and if those were being captured by the legitimate purpose qualifier that we had earlier, then we maybe we need the whole statement, you know, if you're going to be talking about bots perhaps those are legitimate access; perhaps they're not. But we - that goes back to other discussions about purpose.

So sorry for rambling a bit but I think my basic point is that we have to understand why we - what we're talking about and why we need the statement. And if we do understand both of those things then we need it, otherwise we're just throwing stuff against the wall. Thank you.

Chuck Gomes: So before I go to Lisa and then Steve, this is Chuck speaking, I want to call everybody's' attention to what Lisa put in the chat quite a while ago now, there's been a lot of chat since then. If you scroll up Lisa put a proposed alternative that actually gives a brief and I think simple definition of nondiscriminatory, okay? So it says there, so if you scroll up you'll find it.

It says, proposed alternative, RDS policies for access to thin data must be nondiscriminatory, i.e. RDS policies not be - must not be designed to give any preferential access. So Lisa, I'll now turn it over to you.

Lisa Phifer: Thanks, Chuck. This is Lisa Phifer. Yes, I just wanted to maybe give a little bit of explanation behind where the EWG principle came from, principle that led this group then to think about how it might apply to thin access which was a desire to have a principle that discourages or prevents offering preferential access. By that I mean maybe offering higher rates to certain privileged people, people with more power, people with more money, etcetera.

So the idea was that it be a level playing field, that everybody that should have access to the data gets the same kind of access to the data. And that's where - it was all I guess rolled up into the term nondiscriminatory. But that's

really where the original principle came from, does that still apply to thin data? That's up to this working group, but that was the genesis or the need that was trying to be filled. And I think Michael Hammer had a few comments to that effect in chat as well.

Chuck Gomes: Yes, let's - let me scroll - I'll scroll down to those. In the meantime, Steve, go ahead.

Steve Metalitz: Yes, this is Steve Metalitz. I mean, I like Lisa's formulation if we're going to have anything on this here. But I'm just having a hard time understanding all the objections to people, you know, talking about ways in which this might be presented in a discriminatory fashion or made available in a discriminatory fashion. I thought that we had asked or that Rod and VA had volunteered to get back to us with a proposal on exactly that question with regard to things like captcha and rate limiting and the danger that that - those types of techniques could be used in effect to discriminate or to act as a gate for this data, which we did not want.

So I'm just wondering how this discussion relates to Item 2c on our agenda? I don't know if they have a proposal to present today or not. But I just think we asked them to look into this and so I'm not sure what the resistance is to talking about this now. Thank you.

Chuck Gomes: Thanks, Steve. And let me pick on Rod since he's on the call. Rod, did you and VA make any progress on that?

Rod Rasmussen: Hi, Chuck. Rod Rasmussen here. Only very little. We got questions out to ICANN around their rate limiting and their functionality, which we're hoping to get answers back to this, you know, actually today but we'll see if we actually get those. We do not have any proposal formed yet. We're basically…

((Crosstalk))

Chuck Gomes: So you're waiting for some responses from ICANN staff, is that what I understood?

Rod Rasmussen: Yes, just basically…

Chuck Gomes: Okay.

Rod Rasmussen: …try to figure out what a baseline of, you know, of what they've been expecting from registrars and registries as far as rate limiting goes because this has been in the vernacular for over a decade now. So we didn't want to go and (unintelligible) at the wheel.

Chuck Gomes: Okay. And have they committed to a time to respond?

Rod Rasmussen: No.

Chuck Gomes: And…

Rod Rasmussen: But…

((Crosstalk))

Rod Rasmussen: Yes, no I've been doing double duty with (Andrew) (unintelligible) who's worked - we're actually working on some related stuff there and so he was hoping to get some information back today.

Chuck Gomes: Okay.

Rod Rasmussen: We should have something back. We should have something back in the next couple of days.

Chuck Gomes: All right, thanks. The - all right, let's go to Andrew.

Andrew Sullivan: Hi, it's Andrew Sullivan here. So I mostly - the comments that I put in the response to this you know, were that I didn't really care that much but it seemed to me that it was doing a lot of work. But I'm a little bit concerned now about this suggestion about - that this data always has to be accessible to everyone, you know, at the same rate and without any kind of discrimination and so on.

What I thought we were talking about is the mode in which you're unauthenticated and if you're unauthenticated then everybody who comes in in an unauthenticated way ought to get the same service. And that I'm fine with. But since by definition you don't know who's coming in under those circumstances, there's literally no way in which to discriminate. So I don't really understand the purpose of this item. And that's my original worry.

Now it sounded like from what Lisa said, it sounded like there's this further requirement that nobody ever be discriminated or that no discrimination is ever used in respect of this data. But I think that that's not what we want, right, that we want the possibility of various kinds of enhanced services that could be available to the RDS if you're willing to give up your identity. And since some of this data is going to be - going to be implicated in those kinds of uses, I think we definitely do want people to be able to authenticate themselves and then get the thin data at perhaps a different rate or in bulk or, you know, various kinds of ways.

Maybe you can get sort of historical queries or something like that if you authenticated law enforcement or whatever. But that's all to do with, you know, what happens once you're past the point of entering a gateway. So I'm not totally sure what it was that Lisa was proposing and I'm just nervous about this ambiguity because I'm not sure actually what the consequences of it are. Thanks.

Chuck Gomes: Thanks, Andrew. This is Chuck. And, Lisa, I'm going to let you respond in a minute but let me go to Jim Galvin.

Jim Galvin: Thank you, Chuck. Jim Galvin for the record. Let me kind of reframe a little bit, agree with Andrew and reframe it in the following way. For one, I think I'll open by saying, you know, I no longer support this question, I would say that I absolutely disagree and you know, we're going to need to find a different way to say this to get our point across. The distinction that I think is important here, and maybe this working group was having a little trouble I think drawing this line between what we want in a policy versus what we're going to allow to happen operationally.

I mean, now as I think about this and I listen to some of this discussion, I have to say speaking from the point of view of a registry operator, that has to offer some of this stuff, there's just no way I could agree to this sentence here. There's no way I'm going to let you tell me that I can't operationally, you know, do what I need to do to protect my services. I appreciate the need to have a policy that's nondiscriminatory but to say that I can't put a captcha on things or I can't do rate limiting, you know, for something which is just a broadly open ended service, I think I'm going to have a problem with that. And I think we need to be careful about how far down that path we want to go.

I think that's a separate discussion and that's the distinction I'm trying to draw. Operational concerns are a separate discussion from what we want to be our policy on the outside. And I don't have a suggestion right now for how to draw that line but I do want us to make that distinction. And I'm interested in whether others agree or disagree with that distinction I'm trying to make. Thank you.

Chuck Gomes: Thanks, Jim. This is Chuck. I'd like to call everybody's' attention to the first two words if I count an acronym as a word. It says RDS policies for access to thin data must be nondiscriminatory. So I think, Jim, that the way it's worded covers what you're saying and personally I would hope that that's the case because I agree with you, again speaking from a personal point of view. But

that - those two words are really critical to understanding the statement, whether we decide to leave it or not or accept it or not. This says RDS policies must be nondiscriminatory. That's a different story.

Now if we developed a policy that precluded some of the operational things you're talking about, that would be different, but we would deal with that as a policy. And I'm not predicting that will happen but I just wanted to point that out. So now Michael, is your hand up as well as the green checkmark? I can't - I can only see the green checkmark.

Michael Hammer: Yes it is.

Chuck Gomes: Go ahead.

Michael Hammer: Okay. So I understand what Jim's saying. I believe one of the reasons that legitimate purpose was added in was specifically for the reason of allowing those operational issues to be addressed, abuse, etcetera. But the reality is, you know, when people were talking about authentication, they were talking about filling out a form, things like that, there are other ways of - both weak and strong - of authenticating users. And the problem is when we talk about a policy that's covering registries and registrars, there's always going to be bad actors of various ilks.

And when we talk about policy at the level we're talking about, this presumably will be reflected in the Registry Agreements at some point. It may take a while obviously. And so in a previous discussion, I don't know if it was a week ago, two weeks ago, I raised the point that when we talk about nondiscriminatory for unauthenticated access to thin data, we should perhaps consider not necessarily this statement of policy but to give guidance whereas a requirement that there should be a minimum acceptable amount of resources made available for this type of access.

And I absolutely agree with people who say enabling added value services, bulk access, other things like that, but I think the principle is as long as everybody within a class of access, so if it's bulk access it's the same basis for everybody who want bulk access, not the people who want bulk access should have the same access as unauthenticated users who are using a Web interface. So that's all I got.

Chuck Gomes: Thanks, Michael. Chuck again. Rod, go ahead.

Rod Rasmussen: Rod Rasmussen. So the chat and the conversation is largely caught up with what I was going to say. So I'll just add that, you know, the rate limiting and things like that is a portion of this, it's not the entire thing as far as discriminatory access goes. And it is about figuring out what that line is, right, that is the point of the policy lines so that you don't use the ruse of operational projections in order to actually discriminate against various types of access. That's the whole point of what we're trying to do on the side here is figure out from a policy perspective without getting into the operational side. So it's putting some boundaries around where operations can go rather than telling you how to do your operation. So just wanted to throw that in. Thanks.

Chuck Gomes: Thanks, Rod. And, Lisa, I said I was going to come back to you. Would you like to jump into this discussion especially in terms of the parenthetical that you added to the statement.

Lisa Phifer: Sure, Chuck.

Chuck Gomes: And we talked about yesterday.

Lisa Phifer: Sure. This is Lisa Phifer. So there have been a couple of comments in chat that maybe supersede this but if I can roll it up. The - again, the genesis behind this principle originally was that the access, or excuse me, the policy not give preference to one group of people over another group of people that

- and I should clarify -that have legitimate access to data for a legitimate purpose.

The reason that permissible purposes was in the EWG's principle in the first place, if I recall correctly, was that so let's say everyone that has access for anti-abuse purposes, should be treated the same, that no one in that - with that particular legitimate purpose should be able to pay more money or just by virtue of having more power get preferential treatment when they're accessing data through the system guided by these policies. So that was the original goal.

There's been some comments in chat here about how sometimes providing faster access in return for doing something like authenticating yourself might be a desirable trait. And I'm not - I'm not arguing against it, I'm just giving you the background about why the EWG thought it was important to state that there not be preferential treatment for users with the same permissible purpose.

Chuck Gomes: Thank you, Lisa. And you can take your Xs and checkmarks off of an Adobe if you would like. And I'm going to say that we're going to use a DNS term, put this item on hold and certainly wait until we hear back from the - from VA and Rod on another item that's on hold. Okay? So thanks for the discussion on this.

We're now going to go to the next agenda item which is agenda Item 2b and talk about the principle of proportionality that Nathalie had suggested in a - the poll before last I think to apply for thin data. And a lot of people thought it didn't apply. One of the things that I thought was helpful and staff, if we could bring up the Slide 2 of the handout for this meeting, that would be great.

The - Stephanie in responding to the issue of proportionality and what it means posted what I thought was a helpful chat. And in particular I personally really found it helpful the four test questions that shared on the list over the

past week. You can see the four items in black on the screen on Page - on Slide 2 that's showing right now.

And then what we - what Lisa did after a discussion with the leadership team yesterday, is kind of reworded those to apply for thin data. So I thought it might be helpful if we, you know, kind of answer those questions for thin data the way they are worded, okay, so you'll notice a little modification because the word "measure" in the four tests that Stephanie gave didn't apply as directly probably to thin data and the way we're talking about it. So we tried - what Lisa has done here, with input from the leadership team, was to kind of reword those.

And so what I'd like to do is just ask the group to talk about those questions or - and see. So in other words, if we look at Question A, I'm looking at the red version, is there at least one legitimate purpose for providing public access to thin data? Well, we've already determined that there is, okay. I don't know that anymore discussion is needed on that. One of our tentative conclusions I think says that.

B, is public access to thin data suitable to achieve those legitimate purposes? We can talk about that if you like, is there anybody that thinks that public access to thin data is not suitable for the legitimate purposes? Now we're going to look at legitimate purposes even further, but. And then Question C, and we'll talk about all these at once. Is public access to thin data necessary to achieve those legitimate purposes, that there cannot be any less onerous way of doing it. We've kind of had a lot of discussion about that, I think, maybe not directly so much but indirectly.

And then D, is public access to thin data reasonable considering the competing interests of different groups at hand? And again, everyone's been sharing their competing interests on this. And we want that to continue and I know it will. So I mean, if you look at proportionality in light of these four questions the way they're worded, would it be reasonable to say that

proportionality principle does apply to thin data and going further, that we meet the test of proportionality or will once we finish our work.

Now, enough from me. I'd love to hear from you. Go ahead, Jim.

Jim Galvin: Thanks, Chuck. Jim Galvin for the record. I mean, I guess I'll just jump in and say I think the answer is yes, right, we do know that we need access to this and so I think the proportionality, you know, test does apply. But I think we have answers to all of these questions. So I guess I'm not sure what you're looking for here in the working group discussion, you want me to try to answer A-D or are you looking for something other than just support here?

Chuck Gomes: You did what I wanted, Jim.

Jim Galvin: Okay thanks.

Chuck Gomes: That's fine. Okay. Jonathan.

Jonathan Matkowsky: The principle of proportionality is a privacy principle with respect to personal identifiers that are outside the scope of thin Whois and therefore to use that terminology when it doesn't apply - the personal identifiers is confusing in the context and leads people to mistakenly believe that there are issues that are stake that really have no place here. Thank you.

Chuck Gomes: So, Jonathan, so that's exactly why I thought looking at proportionality - at these four tests was more helpful than looking at the abstract principle of proportionality. When you look at these four tests, it seems like it's - like Jim I think just said, is that yes, proportionality applies to thin data. And what we're proposing meets the tests of proportionality. And, Jim, that's kind of what I was getting at. Instead of asking does the principle of proportionality apply to thin data, I was saying do these four tests - are these four tests satisfied in the direction we're going for thin data? That's - those are two very different ways to ask the question except I think the latter is a lot easier to answer.

Greg Shatan.

Greg Shatan: Thanks. It's Greg Shatan. And I share Jonathan Matkowsky's concerns here. If the principle of proportionality doesn't apply here there's no reason to apply the tests. And applying the test, even if there are questions that we can answer in the affirmative, implies that the principle of proportionality will be applied to all that we do regarding thin data. And again, this was a concern that we're looking at the questions so narrowly that the downstream effect of saying now that proportionality applies is, you know, could have unintended consequences.

You know, perhaps we could say assuming for the sake of argument that the principle of proportionality would apply, you know, can we satisfy the test for it without acknowledging in any way shape or form that the principle itself actually does apply, then we could answer these questions and we could also, you know, answer four questions about our favorite cheeses, which would be equally - hopefully the answers would be equally positive and equally irrelevant. Thanks.

Chuck Gomes: So, Greg, throw the word "proportionality" out and just answer the questions for these four questions in red.

Greg Shatan: I can't do that because the reason that these questions are being asked is to see if we satisfy the principle of proportionality. It's like trying to tell somebody who's afraid of…

((Crosstalk))

Greg Shatan: …that as long as they look at the…

((Crosstalk))

Chuck Gomes: If you can't do it that's fine, let's not ramble, okay? That's fine, I asked you that, you said you can't do it, that's what I wanted to hear. Michael, you're next.

Michael Hammer: Okay. So we have an assertion that the principle of proportionality is fundamental to this even though it doesn't appear in directive itself. And so I've been doing some googling of various law sources from within Europe, so for example, (EurLax), which is access to European Union law. And what I find for proportionality principle is that it regulates the exercise of powers by the European Union, it comes out of Article 5 of the treaty on European Union. It says nothing as far as I can tell that would apply this to what we are doing.

So I have to ask, seeing as it's being asserted that it applies here, that those who are making that assertion provide citations that would support that assertion.

Chuck Gomes: Okay, thank you, Michael. Stephanie.

Stephanie Perrin: Stephanie Perrin for the record. And it is very convenient that I'm up right now because I think I can supply some rationale for the assertion. First of all, as Mr. Hammer has pointed out, this isn't part of the data protection directive, it's principle of interpretation. Caveat again, I'm not the lawyer here and I'm always hesitant to lecture the lawyers on law.

However, it's important principle in terms of regulatory action and public acts, and this is a public directory that we're talking about. And what we're discussing right now is indeed the minimum data set that we believe should be - not should - must be accessible to everybody. So I do think that the proportionality principle is something that applies. And I also think that when the data commissioners get around to investigating a complaint, or the matter goes to court, the proportionality principle will certainly be brought into examination. So I don't think it hurts.

Furthermore, I think these objections are basically on principle that nobody wants to think about the proportionality principle because it applies broadly to our entire activity here, and that's why there's such strenuous objections because I believe that thin data passes the proportionality principle. The only data element I've got any particular questions about, and again, besides not being a lawyer, I'm not a registrar or registry working with these data elements and setting up systems and dealing with traffic on a daily basis.

But I do question the expiry date. I think that's where the third - or the fourth test about competing interests might not be met. But other than that, I can't see why you would not accept the proportionality principle as a means filtering what we're doing. And we can pat ourselves on the back and say, yes, it looks like providing this data in a public directory seems like it passes the proportionality principle. Thank you.

Chuck Gomes: Thanks, Stephanie. And clearly there are some people who have real fears about applying the principle to thin data so I want to recognize that. Andrew, go ahead.

Andrew Sullivan: Hi, it's Andrew Sullivan. I may have said this in the chat, I don't know if I said it may be clearly enough though. It seems to me that you could take this thing, and for those who don't think that there's any data in thin data that could conceivably be covered by this principle, and you can then follow that path and say there's no data in there so the principle doesn't apply, for those who think the principle does apply, the answer to these questions very clearly says in any case that we're going to do exactly the same thing as though there was no relevant data covered by this principle in there anyway.

And so regardless of which side of that fence you find yourself on, the answer is exactly the same one. And so we don't actually have to care why we end up with this result, the answer is the same for thin data regardless. And I think what we should do, therefore, is declare victory and move on to something

that is more challenging than this because it's very clear that we all agree with the outcome and we don't - and precisely why we get to that agreement doesn't have to matter, I think.

Chuck Gomes: Thank you very much, Andrew. That's where I was headed as well. And you stated it better than I could. Yes, I don't think that it's, you know, I don't think it's worthwhile spending any more time on this particular issue. We've had a good discussion, but I think the result is the same, whether we think that the principle applies here or not.

Certainly as we move forward we may have to deal with certain aspects of it and discuss that and we will. So my suggestion is that we don't add the principle, but that doesn't mean that the elements of the principle may not apply as we work - continue our work further. Are there any objections to that action?

Okay, and again it's hard for me to listen closely, which I really try to do and stay up with the chat so apologize for that. Stephanie.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. And again, I'm going to bring up something I've mentioned many times but I'm going to do it again. Most data protection law does not talk about personally identifiable data; it talks about personal data. And persona data relates to a file or a series of actions of an individual and if you take a subset of those actions and put them out without the identifier, that does not deprive the data of the character of being personal data because it came from a personal file and you can link it up. And the expiry date in the registrar is probably enough to get you to link it up in some cases, I don't know. But we haven't really debated the link-ability of thin data with the individual here.

So it's personal data, it's just not (unintelligible) on it. That's one of the other reasons why applying the proportionality principle to a public directory display of that data is an important thing. Thanks. Bye.

Chuck Gomes: Thank you, Stephanie. Jonathan, your turn.

Jonathan Matkowsky: I think that we have debated whether or not there are identifiers within the thin Whois data that could be linked to other identifiers that would make data - the data, you know, can be considered personal information. We've debated it at length by email and we were stretching our imaginations down to SLA records, and found that there was no personal identifiers. So I strongly disagree that the rule of proportionality applies to thin data.

Chuck Gomes: Okay well we're going to stop talk about the principle now. We obviously have disagreement whether it applies or not. But again, I think we can make progress without reaching full agreement on that idea. So we will not, for now at least, and maybe never, include the principle of proportionality but it's certainly generated some healthy discussion. So I want you to scroll down to the next slide on the screen, Page 4, or excuse me, Page 3. I was already on Page 3.

So and I'd like you to - we've been promising for weeks that we would examine the data elements that - the definition that we assumed for thin data and they're over on the right there in that orange box, okay. And three questions to throw out. Are the gTLD Whois registration data elements that we have classified as thin, sufficient at this time? Are any elements listed here not required as thin data accessible through an RDS? And Stephanie, I think has already identified one that she thinks fits that category.

And three, are any new elements required as thin data elements to be accessible through an RDS? So we're finally getting to that question, actually we broke down into three questions, to see if we can reach agreement not just assuming what the thin data ones are, but can we reach at least rough consensus on the elements in the thin data sets?

Jonathan, is that a new hand? Okay. Jim, go ahead.

Jim Galvin: So thanks, Chuck. Jim Galvin for the record. I guess I'll make two comments. One, data not to include. It's not clear to me, I'm interested in some discussion as to why status information and date information need to be included as part of thin data. So I'd like to hear some of that. And then the other thing is I'd like to suggest that DNS SEC information be included as part of thin data because similar to the name server information, you know, this is public information anyway, it's in the DNS. And it's useful to have it as DNS data - useful to have it as thin data. It provides a nice out of band mechanism to confirm the information in the DNS. And it's no more exposure than is already present because it's already public information. Thanks.

Chuck Gomes: Hey, Jim, before you go away, this is Chuck. For those who don't know what that would mean, we obviously don't have it on the screen as an example, what would the DNS SEC information show?

Jim Galvin: The key data, so it's either the key - the DS info, which is available in the TLD zone. So I'm talking specifically about the DS record information.

Chuck Gomes: Thank you. Okay, Andrew.

Andrew Sullivan: Hi, it's Andrew Sullivan. So I strongly agree with Jim that for the very same reason that name server data is in here, the DS records ought to be as well. And I think that's an excellent idea. The reason that the status stuff and the dates are needed is for troubleshooting. So if I am working with another network, and I suddenly start getting, for instance, problems connecting to them, or so on, one of the things that I can do is check in the Whois to see whether there's a problem.

And so for instance, if I am working with oh, just for example, large software provider based in Seattle, and I find that the created on date for a domain that I was using to communicate with them only yesterday is today's created on date, that gives me a pretty good explanation of why I'm having problems

communicating with them because what's happened of course is that they've lost control of the domain and somebody has jumped in and created it. This is not an entirely fictional example.

So I think that that's the reason to have those dates there. The same thing is true of the status value. If I discover that the status is hold and I can't send an email to the domain, that's not too surprising because hold of course tells me that the domain should not be in the DNS. And if there are enough name servers there, but there's a hold, that would - that gives me a reason why the name is not in the DNS.

Now of course it doesn't tell me - it doesn't tell me why that has happened but it does tell me what the technical conditions are so that if I'm the poor grunt on the help desk and, you know, the senior vice president is calling me up to ask why this is happening, I have an answer to give them so that they will go away so I can do the continued debugging, whereas if I have to say I don't know, then, you know, that poor person on the help desk then, has a bad day because they now have two problems, right, they have this other site that is not working for them and also they have senior management asking them why they can't answer questions.

Chuck Gomes: Thank you very much, Andrew. Good response to Jim's question. Marc Anderson, your turn.

Marc Anderson: Thanks, Chuck. This is Marc Anderson. And I guess I'll just refer to what Lisa Phifer just put in chat. She actually made the point that I was about to make, sort of the example on that slide maybe isn't a current example of thin data, you know, today's thin data, you know, I think traditionally or I guess today's thin data now does include DNS SEC, but it also includes the registrar abuse contact email and phone number.

You know, I sort of, you know, from a personal perspective, you know, I question whether that's a domain attribute and not a registrar attribute, but

the fact remains that's part of a thin response today and so I think we should include that in our deliberations. Thank you.

Chuck Gomes: So, Marc, Chuck speaking. So you would recommend adding the abuse contact information to the thin data?

Marc Anderson: Actually, I wouldn't. I'm pointing out that it's part of, you know, it says example of today's thin data elements, but an actual example of today's thin data elements would include the registrar abuse contact email and phone number.

Chuck Gomes: Okay. So you're just pointing out that the currently thin data includes more than we have in our example. Keep in mind the example went back to a Whois working group many years ago and (unintelligible) that definition. So what we're - so that's fine. So you're not - I just wanted to be clear, you're not recommending those be added, you're just pointing out that there are some additional thin fields that are in there today.

Marc Anderson: Exactly.

Chuck Gomes: Okay that's fine. So now I'm anticipating, if there are no objections, that will - that our poll this coming week we'll start getting a feel for some of these things. Now so Jim has - Jim, you have - sorry to pick on you but I think it'll help us moving forward, you asked for why status and so forth were in here. And Andrew gave his perspective on that. Do you still think those should - certain fields should be removed? And would you like more explanation as why they should be there?

Jim Galvin: So, thank you, Chuck. Jim Galvin for the record. In addition to Andrew's comment, I want to call out what Stephanie said in the chat room and, you know, make the observation that one thing to consider is that the expiration date is, you know, directly related to choices that (unintelligible) is made with respect to registration so therefore it's as it relates to a person which might

suggest that that might be more related to being PII. And so that does raise some questions as to whether even that should be there.

I guess I don't have a firm answer at the moment. Andrew obviously makes a valid point with respect to status information and so does Stephanie. And I don't know quite how to reconcile that in my mind at the moment. I'm still listening to see where I want to go. Thank you.

Chuck Gomes: Okay. Thanks, Jim. And Stephanie, if I can get clarity from you was it the expiration date, because I'm envisioning some of these being questions to put in our poll. Am I remembering correct that you suggested that the expiration date is - be removed from thin data? Stephanie, you can go ahead and respond. Or did I mix that up?

Stephanie Perrin: Stephanie Perrin. No, thin data is one of the data elements that I wonder about whether it's okay to release it. I think there are arguments about that expiration date, for instance, if the expiration data is out there in terms of my domain, then the domain, if you can track me down then you can start sending me spam about grabbing my domain and renewing it, transferring it over, etcetera.

So unless people really need the expiration data for the functioning, why is it out there? You know?

Chuck Gomes: Okay.

Stephanie Perrin: So in other words, looking at this as all personal data relating to my file, my choice, my registration, even the assigned servers, and all of that stuff, it's still relating to my file, just like if I have a telephone subscription the fact that I go to one company over the other is my personal data and (unintelligible). So the question is, what's sensitive to release and where is there an overwhelming need to release? And this is the (unintelligible) I can think of, that I question.

Chuck Gomes: So I want to be clear, Stephanie, and then I'll get to the other people in the queue. So your recommendation would be that we remove the expiration date from thin data, is that correct?

Stephanie Perrin: Unless someone can give a really clear reason why you need it out there, yes.

Chuck Gomes: Okay and of course people are welcome to…

((Crosstalk))

Chuck Gomes: That's all I needed. That's good. Michael.

Michael Hammer: So I find Stephanie's argument about expiration date being personal data and why put it out there is interesting because in actuality creation date is much more personal because it is explicitly chosen by the individual registering the domain and it is much more unique than expiration date because expiration date will always be some multiple of a year when it's created.

So I believe that all of this information is important and useful. It's used on a daily basis by folks in the anti-abuse space. So while it may be personal in one sense, I think in the sense that it has been shown over the years, or even decades, to be very, very useful in the operation of the Internet at large.

Chuck Gomes: Thanks, Michael. And I want to point to everyone, and this has been said many times over the last few weeks, but the question really isn't whether any of the data elements are personal or not, the question is really whether or not we would provide - we've agreed to provide unauthenticated access to the thin data elements. And so what we're really - the question is really whether it's personal or not whether it should be displayed without any authentication because we've already concluded that whatever we decide are the thin data

elements, they will be provided without authentication and without stating a purpose from the requester.

So keep in mind I understand the concern on personal but that's really not the question at stake. So thanks, Michael, for that. Jonathan.

Jonathan Matkowsky: Jonathan Matkowsky for the record. I feel like we're going in circles and I'm having a difficult time following the reasoning here. We started - we reached a conclusion that thin Whois data, which is a term that really is pretty well understood in the (unintelligible) is - should be unauthenticated and available publicly to all. We went through making sure that the principle of proportionality with overwhelming majority of people feel doesn't apply specifically because that term is used as a principle to protect what the data authorities are interested in, which is personal data, however you define it in the various jurisdictions, doesn't apply to thin data.

And we were moving on from there. And now we're going backward and we're saying, well, maybe thin data is personal data and the argument - the example was the expiration date could be the kind of reasoning that, you know, that leads to the conclusion that that's potentially, you know, some kind of data field that needs to be protected, applies to every single piece of data in there. We're opening the flood gates.

You know, the choice that I make of which registrar to use, the characters in the domain name, the list goes on. So you know, I don't - I feel like we should - thin Whois data is what it is whether it should be added to according to the RA standards like by adding the abuse contact, of course that should be done too. None of those fields are personal information. I do think that's relevant because that's how we got to the point where we were talking about unauthenticated access and making it publicly available.

And last point I want to make is that, you know, if you go through each point in the data, you start with any one of them and start listing the types of

reasons that apply for making it available, those reasons arguably could apply to the types of classes of people's interests, while they're connecting to a domain, whether it's, you know, registering a domain that's going to be expired, someone lost interest and backordering, there are so many variations of reasons that people are interested in this data, that you can't, you know, that you can't list all the reasons.

And that applies to the expiration date equally to any other field in Whois. So that's really all I wanted to express and…

((Crosstalk))

Chuck Gomes: So let me explain why we're here. And we're really not going in circles, and I'll try and make that clear. Beginning when we started talking about thin data elements, we assumed a definition from a working group report that was finalized many years ago without ever agreeing with those data elements being in that set. And many times questions have been raised about that and I have every time said we will get there. We will decide. We need to, as a working group, agree on those thin data elements.

We're now doing what I promised a long time ago. We never agreed with this definition except to use it for the deliberations we were doing at the time. So it's really not going in circles, it's finishing something that we intentionally never did before, but we do need to do. I hope that helps. Susan.

Susan Kawaguchi: Thanks, Chuck. This is Susan Kawaguchi for the record. I just wanted to, you know, also sort of pile on here on the use of this information and the fact that almost everything - and this is - Jonathan just said most of this - but are choices and those statuses are choices, you can decide not to lock your domain at the registrar, you know, not prevent a transfer, not select the registry lock. But from a corporate domain name management perspective, you - all of those statuses and all the information in the thin Whois is critical to being able to independently verify what your registrar has done for you.

It may say one thing in your registry account, and then - but in the Whois record, that should be the actual status, that's the way this was developed over the years and that's what we rely on from a corporate perspective.

Also, just to point out again, and I pointed it out in the chat, in the (Nort) Study, Alex brought up the numbers today, 59% were deemed probably legal persons, commercial use of domain names. So we should not be looking at this only as personally identified data because this data identifies legal persons, not just natural persons. So if we need to design two systems, and opt things out for a natural person, that's fine. But I think it's really critical that we put into this the registration directory service what is important for commercial or legal person registration.

Chuck Gomes: Thank you, Susan. Sorry. And let's go to Alan.

Alan Greenberg: Thank you very much. A couple of things. First of all, the question of should this element be in thin data or not I always thought that we were using thin data as an - foolishly as an easy set of data to talk about before we talked about the full set of data. By the time we finish our work, there (unintelligible) thin data. It is a concept whose time will have passed by then in any realistic world of how long our process is going to take. So it's not an issue of being inundated or not, that was just a convenient subset of data. We can talk about whether the data in thin data should be published or not, but that's a different issue altogether though.

Chuck Gomes: Well..

((Crosstalk))

Chuck Gomes: …we have talked about that.

Alan Greenberg: Yes, I'm saying is the question of should it be in thin data is a non-sensible question, it is - thin data is what it is today and some number of months and years from now it'll be gone all together. The issue of personally identifiable as several people have now pointed out, I thought it was an original idea when I came up with it, there's nothing more personal than the character string you pick for your domain name. That makes no sense to say we're not going to tell anyone what it is.

There is - I do feel we are going around in circles despite your explanation, Chuck. Thank you.

Chuck Gomes: Well I don't think - I think is one case where a clear definition is needed. If we're going to make conclusions, and we've made several about thin data, we need to be sure that we're in agreement of what we're including in that definition, that definition, like you say, may change over time, but we need it for that. But we'll agree to disagree on that.

Let's - there was another hand up, it looks like it went down. So I think we've had several suggestions for the changes to this list of thin data elements. We've had a suggestion to delete the expiration date. We've had a suggestion to add the DNS SEC information. And I think we can test those in a poll and the main purpose of the poll will not necessarily reach a final agreement but to facilitate discussion in our next meeting on these so hopefully we can reach some sort of rough consensus or better in terms of what the data elements are when we say thin data. So we're saying thin data elements should be accessible without authentication, we clearly need to be in agreement of which elements are included in that.

The - what other suggestions were made for changes? Now Jim made a broader suggestion and Jim, if you want to leave that on the table, we can poll on that. It's your call. I doubt that we've had enough discussion to satisfy you and I notice that there's been a lot in the chat as well. The - Alan, I'm sorry, but I disagree with you that thin data will cease. Maybe all data will be

accessible via registries, but whatever we define thin data, it's not going away. The domain name, the registrar, those things aren't going to disappear. So I think we're just talking - we must not be on the same wavelength on this.

So, Stephanie, go ahead. You're on, there we go.

Stephanie Perrin: Thanks, Stephanie Perrin. And I don't want to beat this dead horse into a pulp, but we have a fundamental failure to be speaking on the same level here. The definition of personal information has been a subject to debate for decades. There's an exhaustive scholarly literature on this. We have in our document repository, a paper I believe discussing the definition of personal information put out by the Article 29 group.

And Americans who would contest why we should look at the European definitions, I would recommend that they look at - to American scholars on this, one a political scientist and the other a lawyer, Julie Cullen, Configuring the Networked Self and Pricilla Regan, Legislating Privacy, this whole concept of the denaturing of the definition and how difficult it is to deal with once you redefined it has been exhaustively studied.

So I know nobody is going to believe me that this is personal data because it relates to a file initiated by an individual, as Alan just pointed out, to register a domain, but trust me, it is. That doesn't mean you can't release it.

Chuck Gomes: And that's my point, Stephanie, whether it's personal or not, we can still decide to release it. So let's go to Jonathan and we need to close. Please be brief.

Jonathan Matkowsky: The expiration date is absolutely critical information for thin Whois. I would argue that the creation date is much more personal than the expiration date. There's no certain, you know, all registrars like you can register a domain for five years, 10 years, you know, the date and time that I register my domain is much more personal as - in terms of being able to identify me

and my preferences, than when my domain will expire which is set periods of time and absolutely critical information for, you know, for numerous reasons.

Chuck Gomes: Thank you, Jonathan. And Jim, unless you object, we'll go ahead and do a poll question on the fields that you suggested be removed. Doesn't mean that you have to maintain that position or anything else, but if that's okay - okay thanks. Okay good. I didn't want to do it without your confirmation. So we've gone past our meeting time by a little bit so we need to wrap it up.

The - let me give a really brief update on the legal analyses. We, as a leadership team, as we suggested last week and there were no objections, are proceeding with trying to get that started in the month of June so that we can use fiscal '17 funds - fiscal year '17. And the - and Marika, do you want to quickly say anything about the two sessions in Johannesburg?

Marika Konings: Sure. This is Marika. As you may have seen, the schedule has been published and we can post a link in the chat shortly, but the two sessions are now confirmed so on Monday afternoon there will be the cross community discussion on RDS and then on Wednesday there will be the - in the morning there will be the working group face to face meeting. I'll post a link now in the chat so you can find all the relevant information about these sessions and as well as other sessions there.

Chuck Gomes: And again, to emphasize, we did agree to move our working group meeting from Tuesday to Wednesday so if you're looking at the block schedule that was out before, that has changed. So just note that. Anything else that we need to cover? We'll have a poll on some of the data element changes that have been suggested for thin data. Hope everybody will participate in that. And Lisa, anything else we need to cover? Marika? Amr?

Lisa Phifer: I think that's it.

Chuck Gomes: Okay. All right, sorry for going over again. And have a good rest of the week. Meeting adjourned. The recording can stop.

END