ICANN
Transcription
Next-Gen RDS PDP Working group call
Tuesday, 23 May 2017 at 16:00 UTC

Note: 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. The audio is also available at: http://audio.icann.org/gnso/gnso-nextgen-rds-pdp-23may17-en.mp3

Adobe Connect recording: https://participate.icann.org/p27egiiqojz/

Attendance on wiki agenda page: https://community.icann.org/x/HsPRAw

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page http://gnso.icann.org/en/group-activities/calendar

Coordinator: The recording has started.

Michelle DeSmyter: All right great. Thank you. One moment. Well good morning and good afternoon, good evening to all. Welcome to the Next Gen RDS PDP Working Group call on the 23rd of May, 2017. In the interest of time today there will be no roll call, attendance will be taken via the Adobe Connect room so if you are only on the audio bridge please - would you please let yourself be known now?

Beth Allegretti: Hi, Beth Allegretti on the audio.

Michelle DeSmyter: Thank you, Beth.

Daniel Nanghaka: Daniel. Daniel Nanghaka on audio.

Michelle DeSmyter: All right thank you, Daniel. All right, we will note the both of you. Hearing no further names I would also like to remind all participants to please state your name before speaking for transcription purposes and please also keep

your phones and microphones on mute when not speaking to avoid any background noise. With this I will turn the meeting back over to Chuck Gomes.

Chuck Gomes: Thank you, Michelle. And welcome everyone to our meeting today. Let me thank staff for the good slides that they've put up. The first one reminding people to keep up the statements of interest updated, and another reminder that audio is best if you can call in or if you need a callout, that can happen as well. So thanks, staff, for doing that. Does anyone have a statement of interest that has been updated or will be updated? Please raise your hand, and as always if you are not in Adobe, speak up so I can call on you.

Thanks, Michael, for the response to my question. Not sure why it was taking longer today when you dial-in but it did for me so that may be why people are joining late and the numbers are going up in there so that's good. All right, and I don't see any hands for updating statement of interest or hear anyone so let's move ahead in our agenda.

And let's go to the agenda item Number 2. Make sure you do mute your phones, I hear a little interference there. So appreciate that. Now notice that you have scroll control. And in the Adobe window right now are the results for our poll from last week. You can see, if you scroll down, that 25 people participated. And we are going to start with question number 2.

And that question, if you scroll down to page 2 n the screen, and hopefully those of you that aren't in Adobe have copies there on your computer or printed copies of the results.

So we polled the statement gTLD registration thin data must be accessible without requester identification, authentication or stated purpose. And as you can see, we had a strong support for that statement. There were 88% of the 25 respondents supported the statement, three disagreed. And you can see their comments.

I do want to point out that it's understood that we still have to define "purpose" for the thin elements. And a couple of you in your comments, you know, brought a purpose again. And we get that. So we will be doing that in the near term here so I just want to remind everybody of that.

Unless somebody wants to talk about any of the comments or bring up and discuss your own comments we won't go through them one by one. It seems to me that the results on this item are plenty strong enough to declare rough consensus at this point in time realizing that the conclusions we are capturing from week to week are being added to our rolling document that we will have a chance to revisit them later as we continue to make progress.

Vicki, go ahead.

Vicki Sheckler: Thank you. And I was one of the people that objected to the data of record definition. And I…

((Crosstalk))

Chuck Gomes: Well, we're not on that one right now, Vicki.

Vicki Sheckler: Oh, I'm sorry, I thought you were. I apologize.

Chuck Gomes: I haven't - hang in there, we're going to get to that. And I am going to call on you, as you know, on the data of record. I think it'll be very helpful for the whole group to hear you talk about your comments so…

((Crosstalk))

Vicki Sheckler: I apologize, Chuck. That's what I had up on the screen.

Chuck Gomes: Don't worry about it, nothing to worry about. I just wanted to make sure, are there any comments - and you can leave your hand up, Vicki, that's okay. Are there any comments on the results for Question 2? Any discussion or questions? Okay so we have an action item then to add that to our document and it will be one of our rough consensus conclusions.

And as we get into purposes going forward, we're going to find out that the statement is quite pertinent so we will come back to that later. Okay let's go down to Question 3, and pretty strong results here, but the leadership team .it would be important and useful to talk about at least three of the comments that were mentioned in this one.

As you can see the results, 80% of the people were okay with both the reworded statement of purpose and the definition of data of record. But there were I think five comments, and three of them in particular are I think worthy of further discussion. And so I'm going to - only two out of the three of people that submitted the three comments are on the call so I'll try and share some of things from the third person.

But since Vicki raised her hand - now let me go over very quickly for those not on - in Adobe. So the reworded purpose statement was, "A purpose of RDS is to facilitate dissemination of gTLD registration data of record such as domain names and their domain contacts and name servers in accordance with applicable policy where data of record would be tied with a footnote to the following definition. The data set, at a given time relevant to a given registration object, that expresses the data provided in the then current registration for that object."

Now that's a mouthful for those that don't have it in front of them. So maybe for those that do have it in front of you as well. But there were three comments that the leadership team thought, and it's not that we - the other comments weren't fine but the three I think have some questions so I'm going to ask the two people who disagreed with this to read their comment and then

talk about it a little bit. And then we will give everybody in the working group a chance to ask questions or share your point of views.

So let's go to Vicki first.

Vicki Sheckler: Thanks again. It's Vicki for the record. My comment generally was that this - the way I read the definition, update of record, if I understood it properly, they didn't have this concept of the source being a primary or proper source or, you know, the authoritative source as I understood authoritative for the data of interest at the time.

I also read the back-and-forth that Lisa just sent around from Greg Aaron, and I think he talked about, you know, the concept of trustworthiness of the source. I know that we have, you know, said in the past that we want to distinct between whether something is accurate versus whether or not this is the right source you should go to to get the information. This is not a quibble about that distinction; this is more that the data of record definition, as I read it, doesn't include the concept of this is where you go to get the information if there are several sources where you could get it, this is the one that you should rely on.

Chuck Gomes: Thank you very much, Vicki. This is Chuck. Let's let Andrew respond.

Andrew Sullivan: Hi, it's Andrew Sullivan. So I don't have any particular love for this definition. I agree that it's somewhat complex. But that it doesn't have the notion of the place that you go to get it is actually a feature, not a bug. The idea that there is a place that you go to get this data is a mistake, it's a conceptual error in the way that people are thinking about Whois data. There are multiple places - any thin registry today for instance there are multiple places to get the data.

And some of the data is generated by the registry and some of it comes from the registrar. And one of the problems that we've been having is people keep thinking of this as a single data set, as though you go to a place and you get

the official data for a given registration object. But that's not the way the Internet works. And so we shouldn't actually build that architecture into our definitions and instead we should say hey, this could be coming from multiple places but what you need in this data is the data that is true about it right now.

So it is the then current registration for the object, and the idea is that it is, you know, the real current registration for the object, not something that is cached somewhere else or whatever.

Chuck Gomes: Thank you, Andrew. This is Chuck again. Anybody else want to comment? Vicki, would you like to respond?

Vicki Sheckler: Yes please. And Andrew, I appreciate that explanation. I don't think it is a quibble about whether the data is federated or not or whether or not there is redundancy and acquire the data might be located. But more to have a sense of trustworthiness and this is the place or places where you should go to get the data. And that's what I didn't feel was captured in that definition.

Chuck Gomes: Thank you, Vicki. Chuck again. David, go ahead.

David Cake: Right, so what we said, the reason we said not - to avoid using the term "authoritative" is to avoid confusing three different ideas at least. And these sort of criticisms all seem to say well, it doesn't include these other ideas thus illustrating the problem which is that originally this refers to, said, in the data theoretic sense, it is a statement about the operation of the system. It is saying that regardless of federation and caching and all these other things that might be involved in the engineering of a complex system, that's, you know, got to do global service and so on, that it does get you back to the - give you direct access to the most current data within the system.

And that is - the whole point of making the change was to make it clear that that was the case, it was not a statement about where the data came from

outside the system, it's not a statement about the legal authority, it's definitely not a statement about registry versus registrar which is, you know, a very different sort of issue. That's not saying we shouldn't address all of those things, I mean, I think the idea of the, you know, that the data would be trustworthy and the idea that it be dependent on the right legal authority are all very important things to consider.

But I won't just make this change so that we can separate that statement about - this statement about the operation of the system internally, which is a different issue - a very different issue. And the whole idea of moving away from the authoritative terminology was to make it clear that it is a different issue and that we are not talking about those things. So all of these comments seem to be sort of showing why I wanted to make the change in the first place basically, the issue of - as soon as you use the term authoritative we drag at least three different senses of the term in together. Thanks.

Chuck Gomes: Thank you, David. Steve Metalitz.

Steve Metalitz: Yes, thank you. This is Steve. My concern, and I guess it's confirmed by what Andrew was saying, is that I'm not sure it's accurate to refer to the data set in this definition because there could be different data at any given time that meets this definition. It could be data held by the registry versus data held by the registrar or against it could be other differences. But in either case they could be a data set; it exists at a given time, it's relevant to a given registration object. And it expresses the data provided in the then current registration because the registration remains current throughout its lifespan.

So I just think that maybe we need to change "the" to "a" in which case we are more frankly saying that we are not talking about authoritative because there could be more than one data set that meets this definition of data of record. That was my concern about this definition. Thank you.

Chuck Gomes: Thanks, Steve. This is Chuck again. And let's keep that suggestion for the edit from "the" to "a" in mind as we continue the discussion. Always appreciate constructive suggestions so thank you. Alan Greenberg.

Alan Greenberg: Thank you. I'm glad Andrew is up next because at the end of his talk, and I've lost the right word, he used a word like this is the correct data or the true data or something. I don't remember exactly what the adjective was. But that's what's missing here, the reference then current implies this is the correct data, but I don't think it really says that clearly enough, and that's the aspect that I think is missing in this definition or at least is not sufficiently clear. Thank you.

Chuck Gomes: Thanks Alan. Chuck again. And before the turned to Andrew let me remind everybody that with regard to accurate, we are going to get to that later when we get to…

((Crosstalk))

Chuck Gomes: …question. But, no, I understand…

((Crosstalk))

Alan Greenberg: To be clear I wasn't saying it is correct in the sense that someone is lying, but this is the information that we take to be the correct data.

Chuck Gomes: Yes, and I understood you were saying more than what I'm getting at but several times the idea of accuracy has come up in our discussion today. So I just want to remind everybody that we have one of our questions, one of our 11 questions in our charter is data accuracy so keep that one in mind. We are going to cover that. Now back to Andrew.

Andrew Sullivan: Hi, it's Andrew again. So the - there are two meanings of "accurate" here, and that is one of the reasons that we were trying to get away from authoritative,

as David just said a moment ago. The sense of accurate, which is like conforms to the way the world is, like, you know, my actual address is in the RDS or whatever, that's not the sense we are talking about here. What we are trying to talk about is whether you get to the real data that's in the system as opposed to something that's cached, or something that someone has inserted because they have done a man in the middle attack or all those other kinds of things.

So that's what the idea of the then current word here is about. And Alan is right, that's what it's for, but it's not supposed to be - if that's not clear enough then we need to fix the language. But to go back to what we were saying before, the right way to think of this is not to think of it in terms of where you get the data, because we have today technologies on the Internet that allow us to query sources that are not in the canonical source for a given piece of data. And to prove to ourselves that what we are getting is the data that we ought to get if we asked anybody else.

So for instance, what DNS SEC does for the Domain Name System is if you get data from a cache, you can prove that that is the data you should have gotten even if you talked to the authoritative source for the DNS. That doesn't mean that it's correct, right, the account could have been hacked, somebody could have gotten in and redirected it; this has happened to very, you know, to some important domains on the Internet.

But what DNS SEC proves to you is the data you get has integrity, what it proves is that the data you get is the day that you ought to get. That's the idea here of this data of record. What we are looking for is to talk about the kind of data that you get out of this, and that kind of data is what you're supposed to get.

So to respond to what Steve was concerned about, for instance, if there is a dispute between the registrar and registry, or the registry and registrar, about the data, like it could be in more than one place, the question is which one of

them is supposed to be accurate? That's the one you are supposed to get. And if you don't do that then you don't have the data of record, you have something else. That's the idea that we are trying to put across here.

People thought in the recent past people have been thinking that the answer to this is to put it all in the registry and then make the registry the data of record. And that's what thick Whois is all about. But with the pressures from data protection and other sorts of pressures, it's not clear that that is a permanent strategy and instead what we are trying to do is define the data. So if the policy is later changed about where the data is stored or who gets to handle it or anything like that, at the very least we still know what it is we are talking about which is a kind of data which is the real official data, the data of record.

Chuck Gomes: Thanks, Andrew. Chuck again. And, Mark, just before I call on you let me give Scott Hollenbeck a heads-up because Andrew made a - referred to one item that was in Scott's comments and so I will let Scott's come up after Mark and share his comment and talk about that a little bit because it ties into this overall discussion.

So, Mark, it's your turn.

Mark Svancerek: You know, one thing to Andrew, I'm thinking of the word of provenance. Provenance like you would use when trying to determine if a piece of artwork is a legitimate piece of artwork or something. You know, does was owned by the person and before that it was owned by this other person and then it was owned by that person and it was in a museum and da, da, da, da. And you can sort of establish something about that piece of art or that antique or something like that by knowing the chain of ownership of it.

And I feel like data of record is sort of similar to that, right? We know where it's been, we know who signed it, we know who attests to it, who speaks for it

and stuff like that, and so possibly that would be a taxonomic term that we could use to further develop this concept.

Chuck Gomes: So, Mark, this is Chuck, just a follow-up question before I go to Scott. The - are you suggesting a possible edit to this or just using another word to illustrate the meaning?

Mark Svancerek: Oh, well, you know, I hate doing that but if the issue keeps coming up I'm just throwing out the idea that there is another vocabulary word that might be useful.

Chuck Gomes: Thank you. Okay. Let's go to Scott Hollenbeck and then, Alan, I'll come back to you. Okay, Scott, go ahead and share your comment and talk a little bit about it please.

Scott Hollenbeck: Sure. Thank you, Chuck. This is Scott Hollenbeck. I think what you're going to hear me say is similar to what others have already said, and that is the unfortunate consequence of speaking much later in the conversation. But anyway, so my comments, data provided by who? What is the date of record for information that exists in both the registrar and registry? I mean, I might agree with this (unintelligible) point is clarified.

And I got to this comment when I tried to apply this definition to an operational scenario that exists today. We have in the thick registries, contact information that is maintained at both registrar and registry. And the assumption is that they will be consistent. But in the case that they are not I tried to apply this definition, you know, to this operational scenario and I struggled to find a way to determine which of these two representations of the data would be considered the data of record. And so that's why I disagreed.

I think that whatever we do here is we have to come up with a concept that would help us disambiguate the situation of where the data exists in multiple places, it should be consistent but it's not. One of the sources should be

considered more reliable, more definitive, I'm struggling with not using authoritative here, then the other. And so we have a definition that makes that clear I think we need to keep working on it.

Chuck Gomes: Thank you, Scott. This is Chuck again. So, Scott, let me follow up with you as well. So at this particular time is it possible for us to get that much detail? And at the same time understanding Andrew's point that there may not - and I guess Steve Metalitz's too, that there may not be just one source, there may be multiple sources, maybe for the same data or for different data.

But at this particular time until we do a lot more work in our working group, it's not clear to me that we could get that specific at this point in time. Now when we get into developing policies and in particular implementation of policies, phases two and three, I suspect we are going to have to go to deeper, I'm pretty confident we will have to go deeper in this.

So I'm not sure we could do it now though. Do you think it could be done now considering how much more work we have to do and so we really don't know, even like Andrew brought up a centralized registry-based model, you know, now that we are looking at the European Union and other jurisdictions requirements with regard to data protection, that introduces some new problems.

So Scott, before I go to others, is it really realistic to get the level of detail that I think I hear you talking about at this point in time?

Scott Hollenbeck: That's a good question, Chuck. I mean, we've been debating this topic now for several weeks and so I don't know that I'm confident that we could, you know, come to a definition or some sort of agreement in the very near term. But I do think it's critical that we try to do that. Just as I said, if I look at this definition right now I don't know that I agree that the gets us to where we want to be.

Chuck Gomes: And the question is can we get to where we need to be at this point in time or do we need to do for that to a later point in time after we get a lot more of our requirements developed and ultimately develop policy. So, you know, it's a big question. But anyway let's go on and let others jump in. Alan, I assume that you took your hand down, so you're not - need to be in the queue now but…

Alan Greenberg: Yes, that hand was up in error.

Chuck Gomes: Oh okay thanks, Alan. David, go ahead.

David Cake: Yes, I just want to - I thought the idea of mentioning the legal idea of provenance is on the right track of explaining what I think this is - statement is trying to say and this definition is trying to say, you know, we're trying to say is someone querying the RDS will get the information that is currently in the RDS and provably can know that they have done so.

And I think the idea of, you know, is it registry or registration data it all comes back to which is the source of any question we're deliberately this definition does not talk about the source of the data. So questions about registry versus registrar or legal authority for that and all of those questions are deliberately excluded, it's not an accidental one. We, you know, there should be probably made about the appropriate source for each data element probably but that's a different question. And I'm just saying it should remain a different question that we address elsewhere rather than mixing it in with this idea of provenance.

As anyone who's dealt with sort of the, you know, the you know, the idea of provenance, you were just saying that this is the same thing it was before; this is a, you know, the source, the actual source of data could be anything, you know, antiquities, well, I found it in a hole somewhere, it's not - the source is not important, if the provenance says, you know, tracks a thing, and

guarantees that, you know, that you are not begin deluded somewhere along the way but it doesn't tell you about the source.

And that's I think really is the point that a separating the idea of integrity of the data you are getting from the source that originates from is the whole point of avoiding the term "authoritative" or one of the points behind avoiding the term "authoritative." Thanks.

Chuck Gomes: Thank you, David. Chuck again. Now there's been a lot of discussion and chat. And Lisa, it looks like you've been keeping up with that a lot better than I have, I just skimmed a lot of it. But could you maybe not necessarily going through all of them but do a quick summary of what has been going on in the chat? We have a couple people that aren't in Adobe and I think it would help all of us to kind of pull that together, sorry to put you on the spot on that, but if you could take a crack at that I'd appreciate it.

Lisa Phifer: Sure, Chuck. So I think much of what has been going on in the chat relax the conversation that people have been having verbally, but there were two proposed alternatives in chat. One I believe was from Maxim suggesting that we refer to information provided during the last update create interaction; and another was proposed, gosh, I think this might have been from Andrew, that what we are trying to get to here is the data you would get for each datum if you were asked - if you were to ask the source of that data.

Chuck Gomes: Any - on those, any of those jump out as possible alternatives to what we have here? Somebody needs to mute their phone. David, is that an old hand? Okay, Alan, your turn.

Alan Greenberg: Thank you. I've been trying to pull out words that mean - I think the word definitive, to me anyway, means what we are talking about. It is the one that to the best of my knowledge is the correct one and, correct does not mean accurate but is the one from the original source of the data. Maybe other

people read it other ways but I think that is a shorthand for saying it is the data that we take to be the correct data based on everything we know.

Chuck Gomes: Thank you, Alan. A question, I don't know the answer to this, I don't even know if it is a good question to ask. This is Chuck speaking. But does "definitive" have some of the same problems as "authoritative"? I don't know the answer to that but that is a question that comes to mind. So is this - I don't see anybody - got a plus one - you got a plus one, Alan, from Scott and the - there's some discussion about source again, registry versus registrar and as I forget who it was way back up in the chat pointed out that there was, you know, some of the things are assigned after somebody registers a name so they don't really come from the registrant or the registrar necessarily, they might be assigned by the registry.

And Volker suggests most current data. And so lots of ideas going on. I'm wondering if this particular - obviously I think it is the term data of record that is at issue and the definition of that. And I probably should talk a little bit about Greg Aaron's comments which were more lengthy and he was one of those who also disagreed with this. And I will do that after I let Steve and Alan comment. Steve, go ahead.

Steve Metalitz: Yes, this is Steve. My only comment, and it's been reflected in the chat, is that in order to adopt Andrew's suggestion about what the source of the data would say the data was you'd have to design who is the source of each datum. And apparently from the chat again, there could be more than one source for any particular data point. So I'm not sure that that is helpful in disambiguating this or only talking about one set of data. Thanks.

Chuck Gomes: Thanks, Steve. Chuck again. And that's - leads into what I was saying when I was responding to Scott in the sense that we are probably not going to be able to really determine the best sources to go to until we get further along and we seed the design of a system and so forth. But anyway, thanks for that comment. Alan, you're next.

Alan Greenberg: Yes, thank you. I'm not sure I'm helping or hurting the discussion but I think the concept we are looking for is not authoritative because that is, as people pointed out, can be misunderstood. What we are talking about is the data that we can take as authoritative. In other words it may be wrong, maybe someone made it up, but this is that data that we have to rely on because it is the best data we have.

So I don't want to get more wordy but I think the concept of taken as authoritative as opposed to authoritative is really where we are heading. The right wording, I'm not sure.

Chuck Gomes: Thanks, Alan. Chuck again. Stephanie.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. I do think that we are confusing this definition with policy goals here and that it might not be the right time to be defining it. But it would be nice if we knew what we were defining. I hope that doesn't sound too ocular, but as we argue about what this really means - I wish Sam Lanfranco were here to defend his idea of data of record because to me we are discussing what I would call quality of data issues at the same time as technical issues of where the heck we're drawing the data from.

And I resist the notion that for instance, even though I was reading the original document for the thick Whois transfer, and the notion that the registry would be the most reliable source of this data doesn't seem to me to be correct. There is going to be a different authority for each data element depending on who is most likely to have the accurate data.

So I would propose to park this in data of record and then we have to figure out what the record is of course, depending on how this thing is configured. And we can worry about what's correct and to the responsible person is for keeping it correct later when we get into the policy issues. Thanks.

Chuck Gomes: Okay. Thanks, Stephanie. This is Chuck again. Let me go to Greg Aaron's comments. And what I did is I asked - because Greg couldn't be on the call today, I asked him to comment on his comments a little bit further and he did. That was distributed, unfortunately with not too much lead time before this meeting. And then I responded - I gave some personal response is to try and get discussion going but not realizing that I wasn't doing that on the whole list, I was doing it just to the leadership team. So my apologies for that.

Greg found a definition, and his focus was really on the definition of data of record. And he found a definition very complex and confusing. And in fact I'm going to read this to you because he reworded it and his rewording is really confusing and makes the point I guess he was trying to make.

He said, "A set of data that is relevant to a set of data that expresses the data provided in the record for that set of data." So hopefully from that rewording you can get some - the gist of what Greg was saying. And you can see that in his comments that were sent out to the working group list a little bit before this meeting.

The - Greg says, "Aren't we simply talking about a registration record that is kept in a specified place? How does a data set express its own data?" And then he goes on from that. And then he goes on and talks about a little bit on accuracy which we will defer. He says, "What does data object mean? And how can we use it if it is not defined? Does it mean an EPP object or an RDAP object? Both or neither? Maybe we should not use it because that conflates data itself with a specific way in which the data is formatted or transmitted yoking our definition to a specific technological implementation."

And he goes on. Certainly we probably need to do some more work at least on the definition (unintelligible) date of record and the definition of that or any other term as have been suggested. Let's let Jim jumping. And we are all hoping, Jim, that you have the magic solution.

Jim Galvin: Well, thank you, Chuck. And with a setup like that I'm doomed to failure I would guess, right?

Chuck Gomes: Sorry.

Jim Galvin: You know, so I've been listening to this discussion and, you know, I absolutely agree with Andrew here. I think that there is an important separation here to be made about policy versus technical architecture and implementation. And, you know, and these can be difficult things to split apart, but I think that is essential that we do that in this context.

So from a policy point of view we clearly have some work that we are struggling to find the right way to define or phrases. I wanted to suggest a slightly different approach for how to think about data of record. I think that's what we're struggling with most, what does data of record mean? And it occurs to me that what we are trying to express is something that's ordinarily, you know, (unintelligible) a security service. And that is in the data, security integrity.

You know, I mean, the point of the RDS is to ensure that you can get access to data of record. I want to know that whatever the registrants told me, you know, when I asked about something I'm going to learn exactly what the registrant wanted me to know about that particular object. And ultimately I think that's what we are tying it to. So we want some integrity. The security service of integrity, as that data moves from a registrant into the system as a whole, however you want to define that system, and in this case we're talking mostly about the RDS, that's the service we're looking for.

And we're trying to not say the mechanism that handles the rest of this. And I don't know if that helps or not but I mean, when I look at this definition that up here I actually kind of liked it when I think about it from the point of view of defining and integrity service. The data set at a given time, right, relevant to a given registration object, it's, you know, the time would be in the assumption

that it's always going to be whatever the registrant wanted me to have so that time that's important here is when they gave it to me.

And it's relevant to the object, it is whatever the registrant wanted to tell me. Andy registration is always current presumably in the system because it just exists in the system based on what the registrant wanted me to have. I mean, it seems to me that the words that are there, at least from a security point of view, express all of the details that you would want to be present.

Now I think I'm going to go along now with Stephanie at this point, you know, may be from a policy point of view some of these terms are overloaded and people are concerned about that. Maybe we should come back to this discussion after a while and revisit it or if people want to respond to my idea that, you know, come out this from a service point of view and it is a security service, that's what's important, that's the most important thing I think we are trying to figure out how to express when we are defining data of record. Thank you.

Chuck Gomes: Thank you very much, Jim. I appreciate you sharing those thoughts. This is Chuck speaking again. And a couple of approaches I think we can take here, one is what Jim liked about Stephanie's suggestion and deal with this later. So we could leave it's essentially the way it is right now with the qualification that we will revisit this later.

Another one using all the good ideas and discussion that has occurred on this call, we could impose on Andrew and David and anybody else who wants to join them to take another crack at this. And I'm sure there are other ways we can deal with this too. Are there any preferences as to which way to go from here? I think we've talked about it enough on this call. That doesn't mean we're done with it.

Anybody have an opinion, you'd like to make in terms of next steps on this? There is a - it looks like Lisa has a data of record definition. Interesting

proposal by Lisa. If all of you looking to chat, and for those that aren't in the chat she says, "How about this data of record definition?" And it goes like this, "Data at a given time can be proven to match the data supplied at the origin for each data element."

Several people keep focusing on the registrant. Notice some of the RDS record doesn't come from the registrant, just keep that in mind. I think everybody understands. Stephanie, I assume you're saying you like Lisa's definition. And Scott thinks that we're getting closer. Jim - we've got quite a bit of support, Lisa, you're doing well.

Okay there's lots of - since we've got an idea for a definition here should we maybe put Lisa suggested definition into a poll for the week, for the purpose not necessarily of finalizing it but - and we may be able to but there seems to be a lot of opinions that we are getting closer. So if nobody objects let's put Lisa's revise the definition of data of record and with the understanding that the purpose statement that has data of record and it may or may not stay the same. If we get a good definition of data of record it probably could stay the same but we can deal with that later.

The poll would just focus on the definition and give everybody a chance to jump in and express their opinion not only those on this call but those that aren't on the call. So anyway so any objections to taking that approach?

Okay, so let's do that. And thanks. This has been not only orally but in the chapters in great discussion going on. And some people still have some concerns there, let's express those in comments and we will try and - we'll get to poll out that includes a new definition of this.

Okay, thanks, again for the great discussion. And let me look back at the agenda. I think that covers the poll results. And at least for me it confirms the value of these polls in moving us forward a little bit and involving everybody

and hopefully getting better each week in the things that we're doing. So everyone's participation is much appreciated in the meetings and in the polls.

All right, let's go to agenda Item 3, which is to complete the liberation on the charter question, what steps should be taken to control thin data access? And it looks like Rod Rasmussen and Vaibhav Aggarwal have not had time to complete their action item to better define "unreasonably restrict legitimate access." So that was out of the statement, "there must be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and captcha provided that they do not unreasonably restrict legitimate access."

And you'll recall that in our meeting last week we decided that that qualification do not unreasonably restrict legitimate access needs more work. So we'll ask Rod and VA if they would continue working this, understanding that bearing very different time zones. VA is in India, if he's at home or near home, and Rod is on the West Coast of the US. So if you two, and I'm looking - and doesn't look like VA is on this call. So anyway but, Rod, if you could follow up with him and kind of get that going early after this meeting that would be great.

Agenda item 3B, we want to look at the charter questions for deliberation on thin data. Okay so if we could bring that applicable slide up now? And it was in the handout for this meeting too. Let's kind of - if everybody would focus on Slide 1 first, okay just to kind of set the context here. And again I'll try and help those that aren't in Adobe.

So the overall question we're talking about is what steps should be taken to control thin data access. Okay, and the thin data elements are listed on the slide. I won't read through those. And rough - so far the working group has reached rough consensus on a couple things that are shown there, our Number 20, keep in mind we've been reaching rough consensus for quite a while so we are on 20 and 21 here.

Twenty, is gTLD registration thin data should be accessible without requester identification, authentication or stated purpose. And that's the one that we confirmed rough consensus on today after the poll and discussion over the last couple of weeks. Number 21, there must be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and captcha, and that's the one that we are still waiting on defining unreasonably restrict legitimate access. So we haven't confirmed rough consensus on 21, that's still in the works.

Scrolling down to Slide 2, again you have scroll control. Take a look there and you'll see the main question that I've read twice now into the left. But there are five sub questions, don't worry about the six the question because that's going to be phases 2 and 3,policy development and implementation of our working group.

But let's take a look at those questions for thin data only, and see if we have answered them adequately. So we are going to look at 5.1 through 5.5, the sub questions there. And the numbers correlate as they're shown their correlate to our working draft that we are updating each time we get a new tentative conclusion.

So if you scroll down then to Slide 3, you'll see then the - four of the questions, okay, and what we've done, the leadership team, is we've put possible answers with regard to whether we've answered the question for thin data. So 5.1, should gTLD registration thin data be entirely public? It's our opinion that a possible answer for that is yes, and that's the agreement we reached - we finished today, Number 20, okay.

And I think I'm going to go through all four of these together or at least the first three. 5.2 is how many levels of access to gTLD registration thin data should be provided? Add a possible answer is one, okay, again going back to tentative conclusion 20. And 5.3, should access to gTLD registration thin data

be based on authenticated requester identity? And again the answer here would be no based on our tentative conclusion, agreement Number 20.

Now understand this is especially for Stephanie but really for all of us, we're still going to go through the purposes for thin data elements and agree on whether the thin data elements that we've been assuming are indeed going to stay the same, okay, so we'll get there, okay, so that's a qualification on those.

Let me stop there and let's just talk about 5.1, 5.2, 5.3. Any disagreement with the conclusions - the possible answers on those for thin data only? So thin data should be entirely public, only one level of access for thin data and there would be no authenticated requester. No authentication required of a requester of thin data. Any - and a better look at the chat. I'm looking at the slide - okay, Michael Hammer, go ahead.

Michael Hammer: So Michael Hammer for the record. I have a question about 5.2 when we'd talk about levels of access. So I think most folks know I fall in the spectrum of saying wider open access is better. But do we treat one by one lookups of thin data the same as bulk look-ups if you will? That's really the question I want to ask is if someone is asking for one or two were three that's one thing, but what if somebody wants the whole swath of thin data for registrations in a particular TLD at a given point in time? Is that actually the same level to be treated the same?

Chuck Gomes: That's a good question, Michael. This is Chuck. And it certainly relates to 5.2 and that's - and maybe a relates to the operational controls we're talking about, so somebody wanted bulk information, in other words thin data on a whole bunch of domain names, would there be more than one level at that point or is that even the right way to talk about it? Let's see what Jim has to say.

Jim Galvin: So thank you, Chuck. Jim Gavin for the record. I just wanted to respond to Michael by, you know, clearly stating my bias with respect to this particular topic. I think that if somebody is looking for bulk access, and, you know, maybe it's appropriate to create a line somewhere that fewer than this rate of queries is fine, anything over is considered bulk. I think we should solve that separately.

I don't consider that a level issue. I believe that the word "level" in this context is simply referring to access at all, not quantity of access. So I think that when we want to talk about quantity of access we may want to think about the availability of alternate mechanisms. So that's the distinction I draw, the access itself versus quantity. Thank you.

Chuck Gomes: Thanks, Jim. And let's capture for future reference though, Michael's question because I think it is one - it's an important question. I tend to agree with Jim that this isn't the place probably to deal with that but it's going to need to be dealt with. So that's a future action item, but let's not forget, I don't know how the best way is to ensure that happens but staff will help us out on that I think to make sure we come back. And I'm sure Michael will keep us honest on that to, and we want you to okay. Is that okay, Michael, to deal with it that way?

Michael Hammer: Yes, I just, I happen to believe that when we start specifying, you know, here is a breakpoint whatever, that is a differentiation in level of access.

Chuck Gomes: Okay, and I get your reasoning on that. But, the basic answer to 5.2 is, is that we are really not talking about different levels of access in general. Now with bulk access, change that when we get into how to implement it and how we - how operational controls might be used. We're going to have to get more specific on that.

Okay, let's go to - I should look at the chat. So 5.4, should access to gTLD registration thin data be based on requester's purpose and other criteria?

Now requester's purpose we've already dealt with, right in Conclusion 20. Hey don't have to state the purpose is what we tentatively agreed to there.

Now other criteria like - that kind of gets into the operational criteria that we're still working on. So we still have a little more work to do on 5.4 it looks like. And Rod and VA will come back with some recommendations in that regard for our meeting next week, and hopefully we can get that this - the end of this week so that people have a chance to think about it. Any comments or questions on 5.4?

That brings us then to Question 5.5 which is actually shown on the original slide for our charter as the first one. What guiding principles should be applied to determine levels of access to thin data? And what we've done, if you'll scroll down to Slide 4 or if you're not in Adobe look at Slide 4 in the document that was distributed, what we've done there is we've taken a subset of the principles, okay, the data access principles in the EWG report.

And the reason we took a subset is some of them, especially the latter ones, really have a lot to do with implementation methodologies. But we picked 41 to 46 because they seem to be dealing with where we're at right now. Now again, keep - think of these - so what we want to do looking at 41 to 46, and of course if somebody thinks one of the other principles in the EWG report should be included here, please let us know, but we looked at them pretty carefully.

And the ones highlighted in yellow are the ones we think at least in part, 45, deal with thin data. So 41, 43 - excuse me, 41, 44 and then really just the first bullet in 45 deals with thin - apply to thin data in our opinion. We want you to confirm that you agree with our opinion, that's why all of this is in front of you.

The reason all of 45 is highlighted in yellow is because it wasn't technically possible to just shade the first bullet. So keep that in mind. And I have Michael Hammer, go ahead.

Michael Hammer: I'm just chatty today. Michael Hammer for the record. So I spent most of last week at a meeting that involved anti-abuse people and representatives from law enforcement from a number of countries. And there was some discussion about the RDS Working Group and some of the issues. And one of the concerns that multiple law enforcement representatives expressed was when they are making inquiries or doing Whois queries about domains, having to identify themselves and express a purpose for the request could possibly derail an investigation. So I'm not going to agree, disagree, whatever, I'm simply pointing out that this was expressed.

Chuck Gomes: Thank you, Michael. And I don't think that comes as any surprise any of us in this working group that when we - especially when we get beyond thin data and we're not talking about just public access to some data elements, that's going to be a hot discussion I think and one that will be challenging for us. And then to deal with in - as we try also to ensure that any recommendations we make are in compliance with laws in various jurisdictions so thanks for reminding us of that.

Let's go to Steve.

Steve Metalitz: Yes, hi. This is Steve Metalitz. I would agree with you on 41 and 44 that those seem to be applicable to thin data. I wasn't clear on how the first bullet under 45 would be applicable. Because it says that all data element access must be based on a stated purpose and yet our rough consensus Number 20 says that the thin data should be accessible without stated purpose. So I wasn't - it'd be helpful to get more explanation of how the first bullet of 45 is consistent with that rough consensus point. Thank you.

Chuck Gomes: Thank you very much, Steve. It's a great question and one that we talked about in our leadership call yesterday because I was - even in some of the comments to the poll last week, I was struggling with the same thing you're raising right now. And we came to the conclusion that when we say "stated

purpose" doesn't mean it has to be stated by the requester because that introduces a totally new thing and would go against part of what we said in Conclusion 20.

What - there has to be a stated purpose is the way we're interpreting it, doesn't mean that it has to come from the requester. That's why one of our near term tasks is to agree on purposes for access to thin data as a working group and then ultimately for a new RDS system if there is one so we will need to have purposes that we state are for allowing access. I don't know if I said that clearly or not. Did that make sense, Steve?

Steve Metalitz: Steve. Yes, but I think we would need to revise this point. Now I know we took this from another source so I'm not sure but you would have to revise this bullet point to say something like all data element access must be based on a purpose stated in policy or something like that to make it clear that…

((Crosstalk))

Chuck Gomes: That seems like a really good edit. Anybody disagree with that? Because I think you're right, again, this came from the EWG report so we're not locked into this, it's just a starting point. So I personally liked your rewording of that first bullet under 45. So let's take each of these one at a time. Let's take 41. Is there any disagreement on this call that that principle would apply to thin data the we could agree to that?

Anybody disagree with that, put a red X in the Adobe or if you're not in Adobe just speak up and let us know. And it's fine to put a green checkmark too but in particular we're looking to see if there's any objections to - okay so - and as you have learned with me, I'm going to ask you to explain your answers if you put a red X so that we understand.

So I see one red X and others can still put one in there, but, Michael - Michael Hammer, would you explain why you would disagree with that principle?

((Crosstalk))

Michael Hammer: Sure, I have - the concern I have is most people are thinking of GDPR when they think of the most stringent privacy regime. But how many jurisdictions are there on the planet? So based on this, if a jurisdiction said no data should be published, then is that regime that we want to go with?

Chuck Gomes: Well I think - thanks, Michael, this is Chuck again. And I think this is, in an indirect way, saying no, it's not. It's saying that there should be a minimum set of data elements that are basically accessible without authentication.

Michael Hammer: But it says at least in line with the most stringent privacy regime.

Chuck Gomes: Oh, yes, good point. Michael raises a really important question I think. And again we can reword these, okay, just like Steve suggested on the sub bullet under 45. That clause could be a catch. And Michael brings us something that it's very important for I think - for us to discuss. Steve, is that a new hand? Steve Metalitz.

Steve Metalitz: Yes it is. This is Steve. And I'm just going to agree with Michael that we probably should - I mean, it probably should drop that phrase because I think it's kind of hard to apply that phrase in any context because we would have to know what was the most stringent privacy regime in the world. I don't know what it is. But I think to be consistent with our rough consensus we would want to drop that phrase and just say a minimum set of data elements must be accessible by unauthenticated users. Thanks.

Chuck Gomes: Thanks, Steve. Chuck again. Jim, go ahead.

Jim Galvin: So, Jim Gavin for the record. So I guess I could agree with Steve. One answer is simply to drop that phrase. An alternative that I might suggest that occurred to me when listening to Michael is how about if we were to say - get these words in front of me again here - oh in line with the most applicable stringent - with the most stringent applicable privacy regime, thus, you know, leaving it open for the fact that there's some policy somewhere that's going to put all this together.

I mean, I think the point here that we're wrestling with is just trying to find the right way to say the fact that, you know, there's data that has to be there and obviously we're always going to have to comply with any particular country's jurisdiction with respect to their own data. This is intended to reflect our position with respect to the globally applicable policies, right? And wow, I hope I'm not adding confusion here by just adding more words in this. So I'll just come back to my first point, dropping the phrase, I like Steve's suggestion, or how about most stringent applicable privacy regime, which still gives us the opportunity to define what that is. Thanks.

Chuck Gomes: So this is Chuck, Jim. And regarding the latter suggestion, I would only support that as chair if you agreed to lead the group that's going to define "applicable" because I know that'll come up. So I'm being a little bit facetious, okay. It's not a bad idea. But then we're going to have to figure out "applicable" and we're probably going to have to do with what Steve suggested and figure out what's the most - otherwise we'd have to figure out the most stringent and so forth.

But thanks for the input, Jim. Let's go to Greg and then we'll go to Lisa.

Greg Shatan: Thanks. Greg Shatan for the record. I think I agree with Steve and I don't agree with Jim on this point. I think that that whole clause is a problem especially since, you know, first off why, you know, use the most stringent privacy regime you're essentially forcing everyone to comply. Should we use the most stringent anti-freedom of expression regime in dealing with topics? I

think that's - we would get in a rabbit hole. I think the issue of compliance with privacy regimes I think needs to be considered on its own terms and in its own element or principle and not kind of mixed in to this principle.

Especially since, you know, compliance or being in line with a privacy regime can mean certainly different things based on different elements and different things based on different actors as has been pointed out multiple times. Entities, as opposed to, you know, private individuals have a whole different set of regimes or applications within those regimes with regard to their data. And secondly, being in line with a privacy regime seems to mean one thing to those who are determining kind of pragmatic compliance with the law and those for whom applying it maximally or with the greatest faith in order to achieve a - maybe a larger social objective or something would achieve it.

So deciding how to comply with any regime is - it complicates things intensely. And there can be ways to comply with almost any regime to allow for a data set to be available, so as I am taking that as the case then this is really basically irrelevant statement. Thank you.

Chuck Gomes: Thanks, Greg. Chuck again. And as you know, and I think most everybody else knows, that's why - or part of what you're saying is why ICANN has an exception policy for complying with local laws where you get a very stringent one and that could be dealt with on an exception basis rather than building into a principle like this statement does right here.

Lisa, go ahead. Oh and by the way, I wanted to point out that Jim said he was okay with deleting that phrase in the middle too so I'm sure you heard that but I wanted to reemphasize that. It wasn't as if he was disagreeing with Michael and so far. So Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. I just wanted to provide some context to where that clause came from when the EWG developed this principle. I believe at one time, and those who were in the EWG can correct my memory if I'm wrong, but I

believe at one time we didn't have that at least in line with the most stringent privacy regime as part of this principle.

But after the EWG further deliberated on privacy and came up with principles related to a rules engine and applying sort of a filter on data elements that would otherwise be accessible - a filter based on applicable privacy and data protection laws, through something like a rules engine, I think then we came back and added that clause to this principle to make it compatible with the concept that you might take out from the basic minimum set based on a law that would require you to not make that data public in a particular situation. So that's where it came from and what it was getting at.

I'm not sure how that plays into what we need to do right now. I think someone suggested that this might be something that should be deliberated on separately and I guess that's exactly what the EWG did before it came back and revisited this statement.

Chuck Gomes: Thanks, Lisa. This is Chuck again. And what do you mean "deliberated separately"?

Lisa Phifer: What I meant, Chuck, is that we started - if I'm remembering correctly, we started with a principle that just said a minimum set of data elements must be accessible by unauthenticated RDS users. And then later on, as we came to some agreements on privacy, we then came back to this statement and modified it to allow for the application of the principles on privacy so this wouldn't be in conflict.

In other words, if this statement just said - had just said that there was a minimum set of data elements that would made public without - that is without authentication, then that would have been somewhat incompatible with the principles on privacy that recommended applying some kind of rules engine to possibly remove data elements from that basic set if a particular law required that in a particular scenario.

Chuck Gomes: So I - thanks, Lisa. This is Chuck. So I think - this is just me speaking personally - that what we may need to consider at this point in time, we can, again come back and change it, is whether we believe regardless of the most stringent privacy regime, that there would be a minimum set of data elements that would be publicly accessible. And I guess - I'm not suggesting adding this to the statement, but if then there are some really, you know, rigid jurisdictions those kind of things could be handled on an exception basis rather than letting, as Michael pointed out, the most stringent privacy regime in the world governing everything we do. So which is I think - I'm really glad he brought that point up. So, Jim, go ahead.

Jim Galvin: So, Jim Gavin for the record. Thanks, Chuck. You know, I appreciate obviously this discussion, and it is important to understand sort of these edge cases. But I also feel compelled to remind us that, you know, this system, DNS industry, you know, system only exists because certain information absolutely positively must be public or, you know, there certainly is just nothing that's working and it doesn't exist.

I mean, take for example name server records, I mean, whatever is going to go into the DNS itself, you know, we can certainly have a lot of discussion in jurisdictions you know, can certainly do well. What one might on a technical sense call ridiculous or even stupid as a technical term, the reality is we do need to be reminding ourselves about what data we're talking about that might be excluded from all publication because there is data that absolutely has to be published or the system itself simply doesn't exist and isn't relevant. So I just wanted to make sure we didn't lose sight of that fact. Thank you.

Chuck Gomes: Thank you, Jim. Okay this is Chuck and I'm going to see where we're at as a group on this call. So I'm going to - it's been proposed that we delete the phrase there in - that's separated, "at least in line with the most stringent privacy regime." So it would read, "a minimum set of data elements must be

accessible by authenticated - by unauthenticated" sorry that's big error "unauthenticated RDS users."

Is there anybody on this call that could not support that principle at this point in time in our work? If you can't, would you put a red X in the Adobe or speak up if you're not in Adobe. Okay, Volker, looks like we've got. So in a minute, Volker, I'm going to ask you to explain why you could not support that principle. Any others? And so we've got Stephanie, okay. All right, Volker, let's start with you. Are you on mute? Volker, we're not hearing anything. Okay well we're trying to get that problem resolved because we're running out of time here. Stephanie, would you explain your objection?

Stephanie Perrin: Thanks. As I recall, we were trying to ensure that a data set was clean as it were. And that there were not implications. And I think it just goes back to my thin data qualifier that there - we have to pick a data set that is not going to have to be deleted in a jurisdiction. So and I'm not suggesting this is part of that data set but a for instance is that in Germany employees of organizations have privacy rights so you would not be able to put the name of the tech contact in the data set. You might be able to put tech@acme.de - dotCom, but you could not put the name of the individual. Thanks.

So I'm just not willing to check this out yet. Thank you.

Chuck Gomes: So Stephanie, understanding that we're going to have to go through and agree on the thin data elements, okay, assuming we can come to agreement on what those are, we may, we may not, okay. But assuming we can, could you support this statement with that clause removed?

Stephanie Perrin: I think my argument here, let me rephrase it, it's Stephanie again. If it's thin data it should pass the test so there's no harm in leaving it there. You follow me? Why yank it off?

Chuck Gomes: Not totally because I'm going to go back to what Michael said. What if there's a regime that doesn't allow any thin - doesn't want to allow any thin data to be displayed publicly? That's possible. We want to….

((Crosstalk))

Stephanie Perrin: It's possible.

Chuck Gomes: …drive - do we want to let that drive our position as a working group?

Stephanie Perrin: I think it's unlikely. I haven't found one and I've been looking. I think it's a hypothetical that we don't need to worry about. I think this is a good - let me suggest to you the alternative that you go ahead and assume that it's okay with all data protection regimes in the world and build a system that doesn't allow for it to be suppressed, then you're in a bit of a bind. In other words…

Chuck Gomes: Okay.

Stephanie Perrin: …I think it's a reasonable qualifier.

Chuck Gomes: Thank you. Volker, do you have audio yet? Okay, Tim, you had an X there. Did you want to talk - Tim O'Brien?

Tim O'Brien: Yes, this is Tim O'Brien. I don't think - I think in regards to the privacy concerns and this posting of information, we also have to look at hypotheticals considering what the world (unintelligible) events that are happening. So take case in point with our friend personally doing malware research found the (want to cry) domain and registered it and then you had the sleaze news media in the UK that found out his personal information, his - where he lived and even published directions to his house. This needs to be a - and, you know, the example I was given earlier previously there about hey, this particular company, this person's tech contact, well it can't be its name and just has to be a generic contact.

Well that's already being done with a lot of the domain registrations I looked through, especially more so recently. Not sure why when you have a domain - when somebody filing out or updating their domain registration, that can be given as examples if they need to comply with those policies.

Chuck Gomes: Thank you, Tim. Okay, very quickly, Michele and Greg, I'm going to give you like a minute or less each because we've got to bring this to a close. Michele, go ahead.

Michele Neylon: Yes, thanks. Just very, very briefly, your extreme idea of some - of a regime that wouldn't allow for publication of any data would mean that the domains wouldn't work at all. I mean, technically speaking, as others have pointed out, if you don't have name servers they're just not going to work.

Chuck Gomes: Okay.

Michele Neylon: So I mean, the entire thing with the thin set of - the thin data working on the thin data that's available from dotCom at the moment, you know, that's a minimal set of data that you need in order for a domain name to resolve. So the domain name itself and the name servers without those, the domain isn't going to work. I know Maxim has come up with a hypothetical where you could somehow make it work without doing that, but I think he's just doing that just to troll me, I'm not sure. But, I mean, that, you know, not publishing that somewhere, even if you don't publish it explicitly it's going to end up being published in the DNS in order for the damn thing to work. But having said that, I mean, we're still talking about thin data so in common with others I don't really see an issue with thin data. Thanks.

Chuck Gomes: Thanks, Michele. Greg, you're the last one to comment.

Greg Shatan: Thanks, Chuck. I'll try to be brief.

Chuck Gomes: Greg Shatan.

Greg Shatan: Yes, a couple things. First it's Greg Shatan for the record. As this conversation I think points out that we don't have enough knowledge about the data privacy regimes of the world to really have a sophisticated session about. And that's a problem since we're hypothesizing things that may not exist.

And secondly, when we do deal with data - with privacy regimes, stringent or otherwise, we have to deal with the entirety of the regime including issues - exceptions and limitations and consent and other such things, not just kind of the prime directive. May have many qualifications and ways to deal with it to create a more pragmatic or very variant on the situation. So I encourage us not to look at only the hammer part of any particular data regime. Thanks.

Chuck Gomes: Thanks, Greg. Okay, I'm sorry for going over. Okay, is Greg muted now so that I won't echo? Like Greg and I pair up good together when we're both unmuted. So okay I was hoping to have some sort of a possible conclusion that we might be able to poll on 41. So I think what I'll do just because of lack of time is we'll consider coming up with something as staff so you may or may not see a poll question on this one.

Not for the purpose of probably - a final conclusion but rather to generate some discussion during the week, for those on this call as well as those not on the call to facilitate our continuation of this next week. So we will see if we want to do anything there so that's an action item for us. I'm just looking at the agenda. Is Susan still on? Yes, Susan, would you give a very brief update on the CC outreach? Susan, we're not hearing anything. Okay, since we're out of time I won't wait very long. Jump in, Susan, if you get audio.

Okay, what other - our meeting next week is the same time on Tuesday. And what other - Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. Just a reminder that those of you who RSVP'd to the newcomer's tutorial, we're going to segue directly into that tutorial using this AC room once this meeting ends, so please hang on. And a link was posted in chat to the meeting materials page where you can find some slides that we'll be stepping through.

With regard to the action items, Chuck, I wanted to clarify whether you wanted to poll on just the EWG principle 41 or possibly the reworded principles 45 first bullet, as Steve Metalitz suggested?

Chuck Gomes: That's something I want us to decide offline so we don't take more time. I don't have strong feelings. It'd be good I think, to generate some discussion on both of those during the week. But let's decide that offline and via email after this call. And I don't want to take more out of this tutorial time either so but thanks for asking that.

So we have at least the one poll question. And then whether we have another one or two we'll decide that and then just include it for the working group. Anything else? All right, sorry again for going over but great discussion today in the chat and so I appreciate all the thinking going on. And have a good week. And please participate in the poll that comes out and any discussion on the list.

And by the way, when the notes come out for the meeting, if you want to start a discussion on one of the topics in the list, rather than responding to the notes, if you would start a new thread with that topic that would follow the rules we put down a few weeks ago to help us organize things more effective way. So please try to do that. Lisa, is that a new hand?

Lisa Phifer: Apologies, Chuck, old hand.

Chuck Gomes: Okay, all right. Well thanks, everybody. We had a good turnout today and great discussion. Made a little bit more progress as long as we can keep

doing that every week, we'll get there. Meeting adjourned, and the recording can stop.

END