ICANN Transcription
GNSO Next-Gen RDS PDP Working Group
Tuesday, 2 May 2017 1600 UTC

Note: The following is the output of transcribing from an audio recording. 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/EMPRAw

Audio may be found at: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-02may17-en.mp3
And https://participate.icann.org/p3xsdrhcxnt/

Coordinator: Recording has started.

Michelle DeSmyter: Great. Thank you so much Joy, well good morning, good afternoon and good evening to all. Welcome to the GNSO Next Gen RDS PDP Working Group call on the 2nd of May, 2017 at 1600 UTC. In the interest of time today 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're only on the audio bridge today would you please let yourself be known now?

Beth Allegretti: Hi, it's Beth Allegretti. I'm on audio.

Michelle DeSmyter: Thank you, Beth.

Daniel Nanghaka: Daniel speaking. I'm on audio but I will be joining shortly into Adobe Connect. Thank you.

Michelle DeSmyter: Thank you, Daniel. All right, hearing no further names, I would like to also remind all participants to please state your name before speaking for transcription purposes and to please 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 very much, Michelle. Let's start off to see if anyone has an update to their statement of interest? And again, as always, if you're on audio only please speak up. Okay, welcome to everyone for our call today. The agenda is on the screen to the right so we'll jump right in to Agenda Item 2, but please take note of the sub bullet under Agenda Item 1, remember to state your name before speaking and to mute your microphones when you're not speaking.

All right, going to the working group mailing list discussion. I'll ask staff to please put up some rules that the leadership team came up with to try and improve our effectiveness and make it our list discussions something that's sustainable.

Let me start by saying that we drafted these rules after carefully reviewing all of the input that many of you provided as suggestions. The - and we tried to pick out the suggestions that we thought were practically possible. So please understand that we did review all of the suggestions. We didn't adopt all of them, but here are the ones that we have instituted as rules not only for our list discussion but even for our meetings.

Now, first of all, everybody should understand that all of us are expected to follow the GNSO Working Group Guidelines and the ICANN Expected Standards of Behavior, and links are provided on what's on the screen and of course both of those are accessible via our working group wiki.

The first rule, and this was probably mostly goes to us as leaders, is that discussion topics must be narrowly defined. There are so many topics in the work that we're doing and many of them are interdependent, we get that. But the only way we're going to be able to make reasonable progress and effective progress is if we keep our topics very narrowly defined. And we will do our best to do that.

The second one is responses must focus on the narrowly defined topics. So we're going to be - try to be fairly rigorous in enforcing that. Stay on topic. Now the third rule is related to that. It's okay to note dependency on another topic. And to state assumptions made. But then let's wait until we get to that topic before we start debating it and arguing it and so forth. So please understand when we want you to stay on topic that it's okay to note a dependency, there are tons of dependencies, we know that. That's why we keep saying our process is iterative.

We will get to the dependencies and we may have to change something we did when we get there, that's okay. But we're all over the map sometimes on discussions and it makes it very difficult for us to make any reasonable progress.

The fourth rule is that members should be as brief as possible. Please try to follow that. Certainly say what you need to say, share the facts that you have but try to do it briefly because we have - even with just the number of people on this call today, which is at 32 in Adobe plus a couple others that aren't in Adobe, if everyone is verbose in what they say unnecessarily, it makes it very hard for everyone to participate. So please be as - try to be as brief as possible.

Fifth, repetition of points already made, should be minimized. Something's already been said, if you want to put a plus one in chat or something like that or a plus one in the email list, that's fine. But let's not restate things that have already been stated.

Next, members must identify themselves in message text. And the - hold on a second while I mute my cell phone here. Well, I'm not succeeding so it's not very loud. Hopefully it doesn't bother you.

All right, what we are getting out there, we had a huge volume of messages on Thursday for example. For those of us that went through all of those, and just to let you know, per my practice, I did, I didn't make it through the mall until Sunday night, but it is really hard to determine who is saying what.

Now if you can, use email software that will automatically identify you when you do a reply, that's the easiest way. But some of you probably don't use software like that. And so please help us by putting your name or initials or something so that when a string goes on for a little bit we can keep track of who is saying what. I know that's a little bit more of a hassle but it is really a challenge to tell who said what when you're going through strings of email that have gone on for a little bit.

Next, let's make - our approach is going to be, first of all to follow our working group charter. And unless we decide to deviate from that, okay? And as you know we have changed order sometimes, although the order is not necessarily design firmly in the charter, there is an order. And so we may vary a little bit but we are going to follow our charter.

And in our discussions, as we are deliberating, we are going to start with the Expert Working Group report elements that relate to her discussion. That doesn't mean we will end up there, we certainly won't get a lot of cases. But we are going to start there.

For those of you who don't know, so maybe some of the newer members of the working group, there was a huge amount of work by a lot of very smart people with a lot of experience that went into that report. They didn't develop

policy, that's our job. But we are going to start there and do our best not to duplicate work that has already been done.

Now we are going to have to decide whether we agree in certain cases, and we will do that. But our plan is not to duplicate effort that has already been done by the Expert Working Group report.

And a prerequisite for participating in our group, and this isn't one of the rules but it relates to the one I'm talking about, is that all of you have read the report. I know it's long, and we will regularly refer to elements of it so that you can focus on those. But it is essential that everyone read that report.

Next rule, any working group agreements including tentative working group agreements where we reach just what we call rough consensus, like for example using our polls, will be decided by the working group as a whole. Conclusions aren't going to be finalized by list discussion, okay, we will finalize that any working group called and using the polls so that we give everybody a chance to weigh in. You're not going to have unlimited amount of time to weigh in, as you know, you'll have a few days to respond to each poll, and we will follow the practice we have been following for the last few months.

So you don't have to win the argument on the list. Okay? Make your point, and we will consider all input before we reach any rough consensus decisions and of course ultimately when we make final decisions later on in our work.

Next last, if you are going to start a new topic in a thread that's already going on, start it fresh and change the title. Don't just reply about a new topic on one that's already ongoing. And then last of all, if you can, and this won't always be possible but sometimes it will, identify the charter question in the subject line. We've been working on their users and purposes, the data elements and privacy and now we've jumped into gated access, those are the four that we've especially been focusing on the last few months.

Now, I'll pause for just a few minutes and see if there are any questions. Are any of these rules not clear? Greg. Greg Shatan.

Greg Shatan: Thanks. It's Greg Shatan for the record.

((Crosstalk))

Greg Shatan: Hi, it's Greg Shatan for the record. I just would say that, first, they are clear and I think they are welcome and very good in terms of just general hygiene for this type of working group and email list, but it definitely helps to be reminded of them anti-try to be more rigorous about them.

On the second to last bullet point about starting a new topic, I agree 100%, but I think I would just add to that that sometimes it's not so much starting a fresh new topic, although I have seen people reply to totally unrelated email threads from time to time, but it's more a question of when a conversation starts to fork, and then essentially, you know, by degrees, leave behind the original topic. And there may even be two or three forks going on simultaneously from the same topic. I think we need to be conscious of those forkings as well and try to identify even a strain of a topic when it becomes more concentrated on a particular aspect, and not just the complete hijacking of a topic.

Obviously this is one that's not always possible to recognize every time especially as the degrees might be subtle at the beginning, but I think as soon as one recognizes one is about to take the conversation away from the main trunk of the thread, not to mix metaphors, I think it really is helpful to change that heading or start a new thread or, you know, say was, in parentheses, after it and change the topic.

It's not always a bright line but it does end up a lot of times with conversations, you know, that have veered off from the main thread and it

would be good to be able to identify those because from my email software anything that's under a thread just kind of gets buried in that thread and I end up with, you know, 100 or more emails on several different topics that all are nestled under one thread, and I find it hard to, you know, keep up with those subtopics. Thanks.

Chuck Gomes: This is Chuck. Thanks, Greg. You're right, it's not always a bright line. When in doubt, and you identify a dependent topic, it's okay to say hey, I'm going to start a different thread on this even though it's related to this. Anything we can do to help one another be able to stay up with our work will be very helpful. Anybody else have a question or a comment?

Geoff Noakes: Hello, Chuck?

Chuck Gomes: Yes.

Geoff Noakes: Chuck, this is Geoff Noakes with Symantec.

Chuck Gomes: Go ahead.

Geoff Noakes: I had to step away from the phone for just a moment, so by and large all the rules, or the framework that you set out for how we should communicate here, I think are all sort of standard ways that people work.

The two things that I have concerns over is from time to time some of these threads devolve into a very mean-spirited, attack on somebody's character or their intelligence or their relevance. And I just hate it when that happens because then, you know, they're copied to so many people and you have all these replies to it and they just go on endlessly.

So I would like a sense of, I don't know, camaraderie or decorum so that if people have reasonable differences, take them off-line, figure out how to

settle down together and then come back to the mass emailing (unintelligible)…

((Crosstalk))

Geoff Noakes: …in emails over and over.

Chuck Gomes: Yes, you are breaking up a little bit but I think we're getting it all, Geoff. No argument from me on that, I want the same thing you do and so does the whole leadership team. So does, I think, everybody in the working group. Those kind of things are especially covered in the ICANN Expected Standards of Behavior, as you know, and maybe even a little bit in the GNSO Working Group Guidelines.

Let me - I'm going to talk just a minute or two on that though. I'm going to encourage all, certainly I reinforce everything that Geoff said. No disagreement with any of that at all. But I also want to ask all of you to try and be a little bit thick skinned. Sometimes in email something comes across as antagonistic or even mean. And the person may not have meant it that way. All of us have seen people say, well I didn't mean to be insulting, okay.

So on the first hand, let's do our best to do what Geoff just suggested, okay? Be constructive, listen to people, respect it - respect them and talk respectfully, absolutely. But also try not to be overly sensitive. In this world of ICANN, if you're overly sensitive you're not going to get very far. I wouldn't still be in this world if I was overly sensitive, trust me, I would've left a long time ago.

So I just want to throw that out not to minimize anything Geoff said, but to also ask just be a little bit patient with one another too. If you think somebody is being that way, maybe privately say, let the person know that that came across as insulting. If they keep doing it, different story, okay, but be a little bit patient with one another as well. Anybody else want to comment?

All right, well thank you very much and an action item for staff, let's numbered these rules rather than bullets please so that if we want to refer to them it makes it real easy to do, and when we post them on the Website and redistribute them to the list lets number than please. All right, enough on that. Thanks for your cooperation in advance for following these rules.

Let's go now to the next agenda item, which is to continue the deliberation we started last week on charter question, sub question Number 1, and we will bring up some other slides. One of the things, a lot of good suggestions were made besides what we incorporated into rules. And even in what we are going to do right now was in part in response to some ideas that some of you tossed around and you will see those as we go.

I think one thing that I forgot to talk about in agenda item Number 2, one of the discussions or the suggestions that were made is that there be some sort of a primer or coming up to speed type opportunity for new members to the working group or new members to the GNSO or the policy development process.

So before we jump into an agenda item 3 I'm just going to back up a little bit and ask, or let you know, we are going to send out an email asking for people to let us know if they would like to have a session like that, it could be a webinar, it could be a call, it could be a lot of different things. But if there is - we first want to identify the need, and if there is - if there are enough people that would like that, we will do a Doodle poll and find the time or maybe more than one time double cover most people that are interested in that.

So again, that was an idea that came from the group. And we did want to follow up on that. And we will be sending out an email for you to express interest if that would be helpful to you.

All right back to agenda item 3, and we are going to - the leadership team is going to split up responsibilities between a few of us on this. And I'm going to talk just real briefly about the first few slides here. This is from our charter okay, the big question on gated access of course is what steps should be taken to control data access for each users and purpose, and then there are the sub questions there.

And in particular last week, we started on the second sub question, and just focusing on thin data, should gTLD registration data be entirely public or shared access be controlled? And there is a link to this information there as well.

If you'll scroll down, and you have control, to the second slide, the - we modified that question just slightly by focusing on thin data. And we are aware that some people think we should distinguish the two, that may be true. For now we are just - narrow our focus, remember I think it was rule number two, or maybe it was rule number one to keep our focus narrow. And that's all we're doing, okay. Hopefully it won't be long before we get into thick data.

But, I saw a message just before this meeting started saying we should define thin data. I thought we had. We've been working with this definition for quite a few weeks now. And it's there, it's those data elements is why we are using in the working group. Thick data includes other things, and there are some examples of both in the screen there.

Enough from me on this. I want to now turn it over to Susan, let her pick up the bottom of Slide 2. And I'll let you take it, Susan. She's probably trying to get off mute.

Susan Kawaguchi: I am. And I'm a little surprised, I guess I did not follow our call yesterday. I'm not seeing the numbers on these, which one is - I'm sorry for being unprepared. Somehow I missed this.

Chuck Gomes: If you look in Adobe the slide - the Page 2 is there. At the bottom of Page 2 is where everybody should be, answer to 5.1 given by the EWG report. If you are looking at a hard copy there were versions of this that didn't have the page numbers.

Susan Kawaguchi: Okay, I do. I have it now. So what we - the EWG and with a lot of thought and a lot of discussion went back and forth and decided that anyone could make a request from the RDS, but that if certain requirements were fulfilled that you would only receive either public data that's available to anyone for any purpose, or if there is an authentication or verification of your sort of status or who you are, then you could receive other information about the domain registration data.

So in the example we provided, you would receive all the basic thin data and probably a contact ID number for the actual registrant but all of this would basically be the thin Whois data to get anything else beyond that, you would have to provide information about yourself, and maybe that's just a login, there could be different variables on that, or it could be you could have to provide a purpose.

So it's all purpose driven in the same way that we were trying to decide what the purpose of collection and now display, you would need to provide those purposes. And we categorized those, you know, gave different categories which we've actually sort of worked through in this working group, or we've reviewed that EWG's report on the different types of purposes. And there is about 11 of them.

But the, you know, the initial information you would receive without any sort of authentication or verification of who you were once simply the thin Whois data which we deemed was not personal data. And of course an entity that we were speaking mainly to personal data, but an entity you might receive

more data publicly, that's not gated, depending on your status as an entity or personal data.

So sorry for stumbling through this. So and then did you want me to continue on, Chuck?

Chuck Gomes: Sure, this is Chuck. Hopefully everyone recognizes and Lisa and I indicated in the chat, what Susan was just talking about as far as the public data, according to the recommendations of the EWG report, is illustrated on Page 3. Let's jump to Slide 4. Go ahead, Susan.

Susan Kawaguchi: Yes, I don't know why I'm not seeing the page numbers. Even when I zoom out, so okay. So Page 4, I think I'm on that now.

Chuck Gomes: It's the one referring to pages 61 and 62 of the EWG report.

Susan Kawaguchi: Yes, okay. So there are also, you know, you could see in this image that there is, again a possibility of receiving additional information, what we are probably most familiar with, calling it a thick Whois, you know, the actual contact information, the address, the email address. But with that you must be accredited and you must receive a request or ID.

So that accreditation could be, you know, there's different levels of accreditation we could use. There is different ways of authenticating and who would do that, but you could, once accredited and authenticated, then you could request either the registrant information including, you know, the name of the registrant, the address, email address, and telephone number, whatever information we have decided to include for the registrant in this database would be available to you based on a purpose.

And also with some, you know, each person that was - each requestor that was accredited and obtained that requestor ID would have to then, you know, agreed to terms of service. We all know it's hard to enforce in terms of

service but I think it's worthwhile and people would be responsible in using this information and not, you know, doing something that's not allowed for the terms of service, so there is some controls. So you can see that in the diagram. It, you know, you may be able to receive additional information than just the thin Whois.

Chuck Gomes: This is Chuck. Susan, I want to jump in just to point something out that's kind of a carryover from our meeting and discussion last week, and maybe even a little bit on the list afterwards is I believe, and Susan and others on the EWG can correct me on this, I believe that the Expert Working Group assumed that the public access would be anonymous access.

It's my opinion, and its working group can change my opinion, okay, but in my opinion if we wanted to as a working group we could decide that even the public elements don't have to be anonymous access. We could at least require somebody to identify themselves with an email or something very simple. It may not be authenticated like the gated access that the EWG report talks about. But that's a possibility.

I only throw that out because it was a follow-up from the discussion last week. We don't necessarily have to - of course we don't have to assume anything in the EWG report, but I think we would be negligent, and if we didn't take the report very seriously and take advantage of the time that they spent. So this does not - we don't have to assume anonymous access for any elements we decide should be public. Go ahead, Susan, if you have anything else.

Susan Kawaguchi: Yes, I would just say I agree with you on that, that we, you know, obviously all of the rate limits and those type of things would be in place just like any other access to data. But, you know, and I almost hate to suggest this but if working group members felt that some of the data into thin Whois record, then all the records that we decided - or the contact details should be public, you know, we might be able to provide some with anonymous access

and some of those with a minimum gated access, just okay register to get this information or create an account or something.

So there are, you know, the variables that we could decide to use or, you know, are quite broad. And I think we should, you know, look at those but also not make it so cumbersome that people couldn't get the basic information.

Chuck Gomes: Okay, thank you very much. Let's go to Slide 5 and Lisa is going to expand on some of what we just talked about.

Lisa Phifer: Thanks, Chuck. And this is Lisa Phifer for the record. And so I'll be starting with Slide 5, which if you can't see the page numbers, as Susan had trouble seeing, the title at the top of the slide says, how does this differ from Whois?

So the two slides that Susan just spoke to, their figures that she described, and also the answers that were given by the EWG report, described a number of concepts basically, a number of different concepts that would be used to disentangle data elements that are currently available through Whois and then apply access controls to those.

So what I'm going to try to do is lay out the terminology a little bit more piece by piece so that we can use the terminology may be too guide our discussion and deliberation within this working group about whether all data should remain public or whether some thin data should be placed under some level of access control.

So asked Susan mentioned in that EWG report, the data elements that we see in Whois today were split into two pieces, and they aren't really exactly thin data and thick data, as the two pieces. They are the minimum public data set, and then gated data. So what the EWG report is carved out a subset of all the data elements that exist today and that were recommended as additions into EWG report and identified a minimum public data set that does

include the thin data elements but it also includes some additional data elements, that I won't really go into here.

The idea though is that there would be this minimum public said that would be available just as it is though Whois today, that is available to anybody for any reason, they don't have to state a reason and they don't even have to authenticate themselves, although they can.

The rest of the data, and that would be the vast majority of data including all of - virtually all of today's thick data elements, would be gated. There isn't just one gate in the EWG report, actually there are multiple gates and each of the gates are based on policy, and it is a policy associated with purpose and the data it needed to satisfy a particular purpose.

So how would you get to data into EWG's model? Well, isn't that EWG's model is possible to get to public data without identifying yourself, without authenticating yourself, only getting to that minimum public data set. However, if you want to, you can authenticate yourself even for that minimum public data set but you must authenticate yourself in order to get to any gated data.

So why authenticate yourself? Well of course part of it is to provide accountability to requesters, but part of it is to associate a particular requestor with a purpose that they are actually accredited for. So in the EWG's model, users would be accredited for one or more legitimate purposes, and once they are accredited as having that purpose, that legitimate purpose, they are authorized by policy to access of course the public data set, but also some gated data; gated data that's associated with that particular purpose and gated data that would be also then subject to applicable law.

So it's not just that you get through the gate, because you have a particular purpose and now you have access to everything for that purpose in the EWG's report, there was a concept of actually whittling down that gated data

in accordance with applicable law. And if you read the EWG report it was referred to as applying a rules engine based on applicable law.

Now what does accreditation means? Accreditation could vary by each of the purposes. The EWG's report didn't go into as much detail on accreditation as it did on some of these other concepts because frankly we realized that accreditation might vary by purpose and might be carried out by different portions of the community. And so it was identified as an area requiring further study at the end of the EWG report.

But, part of the idea there was that accreditation might vary based on the risks associated with the data elements being accessed for that purpose. For example, you might have self-accreditation for a purpose that gets you only to pretty low risk data. An example of that might be technical issue resolution where you get to some basic contact information for somebody responsible for technical issues associated with the domain name.

But you might have a much higher bar, you actually have to go through third-party accreditation for purposes that have access to very high risk data. And again that accreditation would depend on the purpose, not necessarily what accreditation gets you into data associated with every purpose, but for each purpose that you applied, and demonstrated you had a need for that data.

So the bottom line here is that there are several concepts, kind of a taxonomy of access controls laid out here of identifying yourself, authenticating yourself, being authorized access particular subsets of data where everybody can get to the minimum public data set but only those who are authenticated and authorized for a particular purpose could get the data elements associated with that purpose.

I would like to mention, because it was raised on last week's call, that the anti-abuse measures such as rate limiting, they would apply to both data sets, to all kinds of access. And rate limiting wasn't the only anti-abuse

measure identified in the EWG report, but that would be orthogonal really to this taxonomy of access controls. And it would apply across the board.

Now that doesn't mean you might not have different rate limits apply for different purposes of course, but the concept of actually using rate limiting to deter abuse would apply across the board.

I'm going to move forward to Slide 6 and to show you a graphic depiction of this taxonomy.

Chuck Gomes: Lisa, this is Chuck. Could you give an example of a high risk data? I think you already did, but Paul asked that in the chat I believe.

Lisa Phifer: Sure. Sure. So if you'd read the EWG report section on privacy and data protection, you will see an examination of several different ways that data protection laws and privacy laws might be accommodated. The EWG's recommendation for that was to develop a rule then that would depend on the jurisdiction associated with the parties involved in the transaction and might then take certain data elements that would otherwise be accessible, might hide them in accordance with the applicable laws.

And a really good example of that might be an individual's name, and individual's phone number for example, those might be considered higher risk than something the technical contact's email address which is considered lower risk because there are ways that of course we can all filter out spam, so there are ways of dealing with some of the abuses of that particular data element, and also there is a relatively strong expectation that if you are listed as the technical contact for a domain name you are expecting someone to contact you and the email address was considered the lowest risk way to contact you.

So that would be one example of how that balance would be struck. But the concept here is that gating would apply to the highest risk data and the

minimum public data that would be the lowest risk data that would be generally useful for many, many purposes to many, many people.

Alright so I just want to wrap up on this last slide and then I see that people are deliberating already in chat. The real goal here was to set up the terminology so we could kick off this deliberation so I'll leave this slide pretty quickly. Just to point out what it shows is the taxonomy here that first you identify yourself, if you don't identify yourself all you're going to get to is that minimum public data set.

Secondly, you authenticate yourself and declare your purpose. If you choose to not declare a purpose or not authenticate yourself you are only going to get to that minimum public data on the right. But if you choose to state your purpose and you are authenticated and it turns out that you in fact were accredited for that particular purpose you can get to the gated data elements that are defined by policy for that purpose. And again that would be subject to applicable law.

Now, these were the EWG's concepts around this, and I think that the kinds of access controls that are laid out in the EWG report are helpful for us to think about what kinds of access controls, if any, is working group would recommend. The idea isn't necessarily to adopt this solution in its entirety but to help the working group members understand all the different kinds of access controls that were applied, to come up with a solution and give us a starting point for our deliberation.

And now I think, Chuck, I'll turn it back over to you with Slide 7.

Chuck Gomes: Okay, staying on Slide 6 for a moment, this is Chuck again. I hope everybody understands that the purposes listed in those, what is it, 6 - 11 boxes at the bottom of that slide are all possible purposes that we could adopt or not or modify, but the EWG report identified each of those as possible purposes for

which gated access could be provide if people were certified for it and had an ID for that. So just want to make sure everybody gets that.

Let's go then to Slide 7, just quickly, I'm not going to spend much time on it. But I want to call your attention to a couple of things there. First of all I want to call your attention to all the links, not that you need to look at them right now, but they are helpful links for what we are doing and what we're going to be doing. Okay?

Two that I want to call your attention to are in the second grouping. You'll see the third will it says, video facts. I'm going to pick on a couple people or at least call their names out here. The video, and it's only 3.5 minutes I think, the first one, does RDS eliminate free public access to data? That was done by Susan, okay? Just a real brief one. And then the next one, what would I need to do to access gated RDS data, is done by Rod Rasmussen. Okay? And I see Rod is on the call today and nice job on that, Rod.

And those of you from the - sorry for picking on you, Rod, and you're welcome to jump in if you'd like, but for those of you in the abuse management role regardless of what that is, hopefully you know that Rod has been involved in that area for I think as long as I've known you, Rod. But that one I think is a little bit longer but still a brief video that I think, I think it's 5, 6 minutes.

And I want to emphasize that there was a good variety of expertise and interest, different interests of people in the EWG. And I'm sure not everything was covered, and Stephanie of course didn't agree with everything that came out of there. But still, there were people from lots of different areas of expertise, some really sharp people, so let's take the work that they did very seriously. And I guarantee will save us a lot of time if we avoid redoing what they are good.

So let's jump to Slide 8 very quickly. And on Slide 8, gets us into our continuing deliberation, and that's kind of the last slide I'm going to cover there. There are some other slides that have additional information, you're welcome to look at those.

If we see that there are questions that come up on those, we will refer to those. But our task now in deliberating in this meeting is should gTLD registration thin data be entirely public or should access be controlled? And we started with this question last week, okay. And there was - there wasn't much - we only had two objections in this regard. We are going to revisit that question now with hopefully clearer understanding of what we are talking about.

And I'm going to use the wording of this question, okay, but understand that we got hung up last week because probably because it says entirely public. That gets back to the anonymous comment that I said. This doesn't say anonymous, but some people would assume anonymity if it's entirely public.

We as a working group don't have to use the wording that's here right now, although it is one that we are focusing on right now. If there's some way we can modify the question to deal with anyone who has concerns about this please make that suggestion. Jim, go ahead.

Jim Galvin: Thanks, Chuck. Jim Galvin for the record. Just a question, clarification, so entirely public I think what is meant to be conveyed there is for any purpose whatsoever, meaning we don't have to clarify the purpose of the data, this data is appropriate for all purposes at all times. Is that what we mean? Thank you.

Chuck Gomes: That is my understanding, and I appreciate you saying that. Maybe we want to change the wording to say that, I think that would be okay if it helps. Thanks, Jim. Of course if I said that wrong, anybody is welcome to correct me but I believe that is the case.

Jim, go ahead.

Jim Galvin: Yes, Jim Galvin again for the record. I see Lisa typing in the chat room, she added a phrase on what I said, which was without requiring authentication and operate station of any kind, I didn't mean to imply that. And I thought I heard you, Chuck, earlier say that this question does not distinguish whether or not access is anonymous or not. That is a separate question that will be dealt with. Or is that intended to be part of this question? Thank you.

Chuck Gomes: In my - this is Chuck. Thanks, Jim. In my view, anonymity was not assumed, okay, we could make it anonymous or not and still allow it to be public. We just would have some sort of ability to audit, you know, who did it or whatever the purpose was. That was one of the snags I think in last week's discussion on this. And so now, whether or not the EWG assumed anonymity, I'll let the EWG members talked about. I don't think we have to assume that.

And again, if we can be as clear as possible in the question, it's okay to reword this question before we see if there are any objections. So let's spend a few minutes on that. Alan go ahead.

Alan Greenberg: Thank you. For all intents and purposes one can have anonymous access over the Internet, you know, maybe it's not 100% rigorous but for in general it can be pretty rigorous, then asking- trying to identify who someone is, is an access control. So if we are allowing - if we are presuming that there can be entirely public access but you need to understand who it is coming from, then it's not an either or question, it's a three-way question. In my mind, no access control implies you cannot be sure of where it's coming from or who it is coming from.

Chuck Gomes: Okay, Alan. Thank you. So Alan, to follow up, this is Chuck. Entirely public in your mind, and I may be wrong on what I'm concluding, but I just want to

clarify, okay, entirely public in your mind would mean anonymous, is that right?

Alan Greenberg: No, I'm agreeing that's entirely public good required you to state who you are but in that case the alternative is not no access control.

Chuck Gomes: Okay.

Alan Greenberg: The either or implies entirely public is synonymous with no access controls and requiring knowing who something is from is a form of access control.

Chuck Gomes: Yes, thanks. I think I'm on the same page as you, I believe. So Paul, go ahead.

Paul Keating: This is Paul Keating for the record. I hope that's what you meant by Paul, I didn't see another Paul on the list, sorry. I have a question with permissible purpose, and I have an issue about anonymity because we are dealing with thin Whois data here, and there is absolutely no personally identifiable data in this set at all other than traditional volume controls type issues relative to the data provider, why do we care who is accessing this information at all?

I think it should be completely anonymous and without regard to any form I've declared purpose because I personally don't see any personal data in this record at all. Thank you.

Chuck Gomes: Thanks, Paul. This is Chuck. The - so let me ask this question, not seeing any other hands, and I'm trying to watch the chat but I'm having trouble managing the meeting and watching the chat. You guys are really good at chat, I'm not really good at keeping up with it, as you know. So others can alert me to key points that are made there.

So is there any ambiguity in the way this question is worded now that needs to be fixed before I ask whether there is anybody who disagrees - who would answer this question no? Okay, Paul.

Paul Keating: Permissible. I have a problem with the word permissible, it is subjective in nature and subject to subsequent rulemaking.

Chuck Gomes: There is no word permissible in the question.

Paul Keating: Well I see minimum registration data that is publicly available to anyone for any permissible purpose without authentication. I'm looking at Page 9.

((Crosstalk))

Paul Keating: Maybe I'm looking at the wrong…

((Crosstalk))

Chuck Gomes: You're talking about the clarification. I'm looking at the question on Page 8 - on Slide 8, okay? The gTLD registration thin data be entirely public or shared access be controlled?

Paul Keating: Got it, okay, no I have no problem with the question. My apologies to the group.

Chuck Gomes: That's all right.

Paul Keating: I was on the wrong page which…

((Crosstalk))

Chuck Gomes: So I'm trying - we're all trying to be really careful.

Paul Keating: Okay thank you.

Chuck Gomes: Because yes okay. Andrew, go ahead.

Andrew Sullivan: Hi there. Thanks. So you could make this slightly less ambiguous by replacing “entirely public” and saying instead “available without any access token” or “without authentication” like that. Because functionally those two things are the same, and the way it’s phrased does have the problem that some people are saying you could have a, you know, a login that nevertheless allows every single person on the planet to see the same data, but still require a login, and that would be, you know, that would be a substantive change to the model from what we have today where Whois, you know, the access is simply unauthenticated.

Chuck Gomes: Yes, and I think that’s what Jim was saying earlier on.

Andrew Sullivan: Yes, exactly.

Chuck Gomes: Yes, so I’m comfortable with changing the wording. Let’s go to Paul first. Paul, are you on mute?

Paul Keating: Yes, I was, sorry. This is Paul Keating. Maybe the - maybe we should have two questions. First question, should the gTLD registration thin data be entirely public? Question mark. Should that public access be subject to any form of control?

Chuck Gomes: Well…

Paul Keating: Those are two separate questions.

((Crosstalk))

Chuck Gomes: …of doing that. And I may be wrong, so you - I can be corrected. But because I think it is a separate issue to get in - we are going to have to deal with whether or not we want people to login to get it, I'd like to treat that as a - I guess I'm agreeing with you in the sense that is a separate question. But I'd like to focus on this question so that we can probe it.

Now let's get the wording, Lisa…

Paul Keating: But you're asking, I'm sorry, Chuck, you are petitioning a yes or no answer from people that you're asking an or question. Okay, so it's very difficult if people throw their hands up yes to an or question. I'm trying to restructure it so it's not an or question. I think that that's what other people…

((Crosstalk))

Chuck Gomes: Oh I see you're talking about…

((Crosstalk))

Paul Keating: Yes, it's the or that is bothering I think a lot of people because you are asking us to raise our hand, are we in favor of this question. It's like well, I don't know which part I'm in favor of.

Chuck Gomes: Well actually, and I'm going to go to Greg Shatan in just a second, we probably don't need the or if we make the clarification that Andrew and Jim suggested. If I'm wrong on that let me know. Lisa, you want to jump in before I go to Greg?

Lisa Phifer: Sure Chuck. Lisa Phifer for the record. I was just suggesting that a question could be simplified to, should gTLD registration thin data access to gTLD registration thin data be controlled in any way? So rather than giving the two possibilities of public, where people are debating what public means, and controlled access, just ask about controlled access first.

Chuck Gomes: Okay.

Lisa Phifer: Should there be some kind of access control?

((Crosstalk))

Lisa Phifer: And if yes, we can debate which kinds.

Chuck Gomes: Yes, some people may say no though in that anyway. All right, we will continue to deal with that. Greg Shatan, I'm sorry to put you on hold for so long. You're up.

Greg Shatan: No problem, Chuck. Thanks. It's Greg Shatan for the record. I think the issue of anonymous public access versus non anonymous public access and whether that still constitute public access or an access control is a sufficiently important issue that we shouldn't leave anything to assumptions. And I think if you look at the - part of the problem stem from the EWG answer at the bottom of the slide, which says that we are abandoning entirely anonymous access by everyone. And then instead of using the term "anonymous" again, we use "public."

So we say public access to some data with gated access to other data, so it's not - we are not splitting the same hair if you will, between anonymous and non-anonymous or, but rather between public, which itself may be split between anonymous and non-anonymous and the gated, although I would argue that even, you know, registration or lack of requiring a lack of anonymity is an access control.

And I think getting down to words like "token" may be getting a little too far into implementation, because I think we are trying to look at this at a data theoretical level or at least a theoretical level. But I don't think - I think we need to avoid implying that public access means either one or the other,

anonymous or non-anonymous and that, you know, if we either change the sub question, because I think the answer that we are referring to reverse to really three types of access you will, anonymous access, which is, I think we know what that means; public access which we don't really know what that means; and the gated access, which again broadly speaking we know what that means.

But the question is whether public access means the same thing as anonymous access or whether it means something that's the same as gated access, except the only thing you're asking for is non-anonymity, in which case, you know, what does it mean to be public? Are we talking about a public sidewalk or are we talking about public subway where you still have to pay a token, so to speak, to get in.

So I think the bottom line is that we need to be crystal clear, and if that involves breaking things up a little bit more or defining things maybe we need to have or, or, or entirely public, public or subject to an identification or controlled beyond merely non-anonymity. Thanks.

Chuck Gomes: Thank you, Greg. Paul, go ahead.

Paul Keating: I will wholeheartedly agree with Greg's comment that any - control means control, right? It's not a relative concept. If you are a little bit pregnant you're still pregnant. So if you are not anonymous, you are controlling in my mind. So I think the question should be is this data available anonymously? Ok?

Now that being said, any controls on your access as anonymous inquirer are based upon technical control issues. So I want to balance load my servers set so I'm going to limit your inquiry, that sort of thing. Those are completely technical and have nothing to do with who you are, right?

So if there is a technical control, I really hate using the word but, because I'm using it in a circular manner, but if there is a technical reason to restrain your

access in anyway, all right, that is unrelated to who you are, to your identity as a person, then I believe personally that those are permissible for the thin data.

Otherwise, I have an uncategorical objection to any form of control. That includes my meaning to identify myself in any form or substance to this data set, okay, so I believe it should be anonymous, that's what I think public access really is. And any controls should be completely unrelated to who you are, or why you are asking for the data. Thank you.

Chuck Gomes: Okay. Stephanie, your turn.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. Just a query, if we answer this question in the affirmative, does that mean that we are accepting all of the data elements listed on this thin data example here? And I would like to repeat orally what I said in the chat, that there is a difference between personally identifiable information and personal information. This doesn't mean that some kinds of personal information, i.e. data that belongs in my account that was generated as a part of creating my account, that is not per se, inherently personal, such as an expiration date, nevertheless relates to my account and therefore it's my personal information.

That's - you can probably guess which particular elements in this thin data example I'm wondering about scratching my head, thanks.

Chuck Gomes: So, Stephanie, this is Chuck. The way the question is worded right now would be all of the data elements. Now if we need to pull any individual thin data elements out and consider them separately we can do that. So we will come back to that. I haven't read all the chat but I saw that Scott suggested something that might work here. What if we said, "Should gTLD registration thin data be unauthenticated or have unauthenticated access?" Does that work? That kind of leaves out the anonymity issue which I think we need to treat separately. But go ahead, Paul.

And I'll read - I think you're on mute but let me reword that. Should gTLD registration thin data be entirely unauthenticated?

Paul Keating: Okay, so as long - my problem - and thank you, I keep forgetting about the mute button my phone. But as long as unauthenticated means I do not have to identify myself then I'm fine with it. But the problem is once I say that unauthenticated means unidentified, then really it's anonymous, right?

Chuck Gomes: Yes.

Paul Keating: It's the word that the synonym. So unauthenticated means that I haven't verified your identity. You give it to me but I haven't authenticated it. So I'm Scott, it's a good way - it's a good idea for compromise but I don't think the gets us there. I really think that we ought to focus on the fact that we are dealing with a thin set of data elements that are on Page 8, okay, and only that data. And I think that it should be completely anonymous and regardless of who I am or why I'm asking for this data. This should be machine oriented data, there's no personally identifiable data in here.

And I'd like to remind the group, at least I think if I got it correctly is the reason we are talking about all of this is because of privacy concerns. There's no privacy concerns in this data set as far as I know. Ok? Maybe someone could explain to me how there's privacy data in here, but there isn't any as far as I know.

Therefore it needs to be (unintelligible) sorry to say that, but it needs to be anonymous and it needs to be free.

Chuck Gomes: Okay I'll…

Paul Keating: And any form of a control is a control. Thank you.

Chuck Gomes: Alan, go ahead.

Alan Greenberg: Thank you. There is a magic word that was just spoken that directly relates to what I was going to say. I don't think any adjectives, or not sure adjectives or adverbs, like public or anonymous are going to be clear here. For many years public washrooms required you to put some money in the door to actually get the door open but they were still public. We use words in curious ways. And I think if we're - what we're saying is the information is available without any restrictions then we should say that or without any conditions or restrictions, then we should say that and not try to use descriptive words which may have different meanings in different contexts. Thank you.

Chuck Gomes: Thanks, Alan. Paul.

Paul Keating: Paul Keating. I agree with that sentiment, but there are restrictions. And what I'm focusing on, I can agree with your language but, you know, should the gTLD registration thin data be entirely accessible regardless of the identity, without need for identification of the requester or the purpose. I'm happy with that because there are restrictions technically they're going to be applied to this, I mean, there are volume restrictions, there are these kinds of restrictions that are purely technical, that have nothing to do with who you are or why you are asking for the data or what data you are asking for. Okay? Those are neutral conditions that are simply technical in nature, and I have no problem with those.

What I have a problem with is any restrictions that requires me to identify who I am or what my purpose is, or for that matter the data that I'm after other than the fact that I'm asking for it. Thank you.

Chuck Gomes: Thanks, Paul. I think you might have come up with some wording that may work but let's test that little bit further. By the way with purpose we have to be a little bit careful there because we know that poor example in Europe that

anything could be used has got to have a purpose but I don't think that's what you're getting at.

So Paul just gave some wording that might work here. Is there anybody, and we will refine the wording in writing on the screen, is there anybody that would have a problem with the wording he just gave without, and Paul, maybe you should repeat it one more time if you can.

Paul Keating: I'll try. Without regard to the identity of the inquirer or the purpose of the inquiry.

((Crosstalk))

Paul Keating: So it's gTLD registration…

Chuck Gomes: The purpose part might be a problem…

((Crosstalk))

Chuck Gomes: …because of some of the laws.

Paul Keating: No, no without regard to so should the gTLD registration thin data, as we've defined it here, be entirely - be freely accessible without regard to the individual or entity making the request, and without regard to the requesting party's purpose for making the request? (Unintelligible), it's much longer than before but sorry, I'm a lawyer so I tend to…

((Crosstalk))

Chuck Gomes: We won't hold that against you.

Paul Keating: … repetitively redundant.

Chuck Gomes: Okay, all right. Does anybody - and here is where I want you to use, except for those that aren't in Adobe, you can speak up but is there anybody that would have a problem with that wording? We will refine it a little bit more in just a minute, but on first responders, put a red X if there's anything that he said there that might cause you problems in being able to answer this question. Alan, go ahead.

Alan Greenberg: Just that caution that since rate limitation is typically done by IP address, that implies you can't do rate limitation.

Paul Keating: I'm excluding that. That's technical. It doesn't have anything to do, Alan, no it's a great question but it doesn't have anything to do…

Alan Greenberg: I know your intent, I know that was the intent, but I'm looking at just the words. Thank you.

Paul Keating: No, great question.

Chuck Gomes: Okay, Lisa or whoever is controlling the notes, or in the chat either one, yes, that's correct, it was red X if you had a problem with that wording. And I didn't see any red Xs. But let's put the rewording in the chat or the notes, whichever is easiest, okay?

Lisa Phifer: Chuck, the wording is there, red X for the statement, the data should be accessible without regard to the identity of the inquirer or purpose of the inquiry.

Chuck Gomes: Okay thanks. Sorry about that. I read the first part of your statement and didn't look at the last, which is what I was really looking for. Okay. Any - it's in front of everybody. I don't see any red Xs. Greg Shatan, go ahead.

Greg Shatan: Just a concern regarding phrasing. I think the plain meaning is correct but as I'm a lawyer I can think of ways to monkey around with the wording to try to

make it say something different than the plain meaning. And I say without regard to the identity doesn't actually quite say that we are not going to find out the identity. It could mean that you need to identify yourself but we are not going to deny anybody access based on that identity. So I would say it would be without requiring knowledge of the identity or something along those lines to be more clear that we are not just talking about free access to everyone upon showing their identification, but free access without showing who you are. Thank you.

Chuck Gomes: I also think - thanks Greg - I also think we need to be careful about saying free access in terms of monetary free. That quite likely will be what we end up with but we are going to deal with the costs and how to pay for this thing later, so we shouldn't tie our hands. I'm not predicting that it won't be free, please understand me. But I think access without…

((Crosstalk))

Chuck Gomes: Yes. So, Greg, how would you change the wording? So you would say - help us again. Thin data should be…

((Crosstalk))

Chuck Gomes: Are you on mute?

((Crosstalk))

Greg Shatan: Without requiring identification of the requester or something like that. I didn't mean to imply, by the way, by the use of the word free…

((Crosstalk))

Greg Shatan: …some sort of financial…

((Crosstalk))

Greg Shatan: I was implying that there would be no restrictions, which - so that without requiring, you know, the identification or the purpose. Thanks.

Chuck Gomes: Okay.

((Crosstalk))

Chuck Gomes: Sorry, I'm thinking - I'm trying to see the differences. I'm not a lawyer and I'm having trouble seeing the differences, okay? Lisa, you're up.

Lisa Phifer: Chuck, just to point out, this is Lisa Phifer for the record, but that proposal is in the chat, that thin data should be accessible without requiring and inquirer to identify themselves or state their purpose.

Chuck Gomes: And does that work, Greg Shatan?

Greg Shatan: Yes, I was trying to think Lisa, typing with one finger, which was going very slowly so, yes, the answer is yes that works.

Chuck Gomes: And, Paul, does that work for you?

Paul Keating: Perfect. Thank you, Lisa.

Chuck Gomes: Okay. Any other comments before I find out if any - are there - so we've got the wording, and it is the - let's put it in the notes so that people don't get confused as to which chat version is in place. Some notice it is being put in the chat right - I mean, in the notes right now. Without regard to the - I'm seeing a bunch of things put in the notes. I'm confused. Could we have the whole question please in the notes?

Paul Keating: Drum roll.

Chuck Gomes: Yes, they're typing. I'm just waiting for the - I want everybody to be able to see it at once okay? And they're still doing that so be a little patient here.

Paul Keating: I am, it was a bad attempt at a joke.

Chuck Gomes: That's right, you can't see it. I'll read it. Daniel, thanks for reminding me. And I'll read it once they're finished. Still typing, okay. All right, here's what it says, for those of you who are not in Adobe. Should access to gTLD thin data be accessible without the requestor being required to provide his or her identity and without the purpose of the inquiry being provided? Okay. Lisa, you want to comment? Okay, Paul, you want to comment?

Paul Keating: Lisa's was much more elegant. But (unintelligible) she can say things in 10 words that people say in 20. But…

((Crosstalk))

Chuck Gomes: …about elegance than I am clarity.

Paul Keating: I'll live with this, Chuck. I'll live with this, Chuck.

((Crosstalk))

Chuck Gomes: And keep in mind, we can refine these things later, okay? And we probably will. So it's not as if what we're doing is in concrete but I'd like us to make some progress on this. And so now, you still have your hand up, Paul? Is that an old hand?

Paul Keating: Sorry, old hand.

Chuck Gomes: Okay. Now, is there anyone on this call, based on your understanding of this statement, that would answer this question in the negative that you do not

think it should be. So should - anybody would not answer this question yes, would you please put a red X in the chat or if you're - okay, Stephanie. Okay, I'm going to come to you, you know, and ask you to explain. I see a green checkmark, that's fine. So Stephanie, you're the one that would - only one so far at least that would not answer this as a yes. Go ahead, explain yourself.

Stephanie Perrin: I did put a note in the chat…

((Crosstalk))

Stephanie Perrin: …Chuck.

Chuck Gomes: Okay.

Stephanie Perrin: Stephanie Perrin for the record. Basically I'm X-ing it because I'm not sure about the data elements and I really feel I would have to consult my group. I understand, you know, part of the spam we receive through the new domain names from people we really don't want to do business with arises because the expiration date is out there and they can identify who's got it from other names.

So I'm not sure - I'm saying X because of the list of data elements that we haven't necessarily agreed on not of the overall principle. Although I don't see why bots and people who access and people who are doing bulk vacuuming of this data don't want to be identified, what's the problem? Why are they resisting authentication? Thanks.

Chuck Gomes: Okay so Stephanie, remember - this is Chuck - remember that we're only asking each of you to respond in your personal capacity when we do a poll, which we're going to follow this with, okay. So keep that in mind. To the extent that you can get feedback from your group, that's fantastic, it's better of course. But it seems to me that we have strong rough consensus, keep in

mind these are not votes, we have strong rough consensus on a yes answer for this question.

So our action item would be to follow up with a poll that we'll get out quickly, and you'll have until Saturday night to respond. Let me remind everybody, we would like those of you on the call to respond to the poll as well. And we would - and certainly want people who are not on the call to listen to the call and look at the transcript and respond as well so that we have their input before we add this to our collection of rough consensus decisions that we've made.

Now, Paul, you want to jump in?

Paul Keating: I just had a question for the last speaker, which she seemed to - you seem to have an objection as to expiration date of the domain name, can you please explain why that is a concern to whatever group you're representing?

Chuck Gomes: Well let me stop there because we're out of time…

Paul Keating: Oh okay.

Chuck Gomes: …okay? That doesn't mean we can't…

Paul Keating: Okay sorry.

Chuck Gomes: …answer the question. But what I suggest - and I'll suggest this to Stephanie and anybody else, in the - there's always a place for comments in our polls so - and remember to the extent that they're relevant to what we're doing, we're going to talk about those next week after - when we review the results of the poll. Okay? So let's deal with that in the poll itself using the comment box.

Greg, briefly please.

Greg Shatan: Thanks. I'll be brief. Greg Shatan for the record. I don't think this should be characterized as a question of existence by certain people, nor using colorful but somewhat pejorative terms like data harvesters; it's a question about what we are trying to characterize various types of access. I don't think we've gotten to the question of intent or as lawyers like to put it so that nobody else understands what they mean, mens rea. So I think if we just, you know, keep this to the technical aspects rather than implying that people are trying to accomplish purposes, perhaps nefarious, at this point we'll probably get a little further a little faster. Thanks.

Chuck Gomes: Thank you, Greg. Okay, now we're within a couple minutes of our adjournment time. Thanks for the good work today. We will follow up with a poll. I won't repeat what I just said. We want all of you and everybody else in the working group to respond to the poll, but you'll only have until Saturday night, okay?

And these are rough consensus decisions, they're not final votes, okay, we'll get to that at the end of this phase or this half of the phase of our work. The - we don't really have time - well, Susan, very quickly update us on the ccTLD issue. I know you've sent something out, if you'd just remind people what they need to do that would be appreciated.

Susan Kawaguchi: Thanks, Chuck. Susan Kawaguchi for the record. We developed a final list of questions and I sent that out yesterday along with a list of countries we're going to target. And thank you for those that have given us some recommendations on countries and some critique of the questions so the small team will look at all that and take all that information into account. And send it out again with revised version.

Chuck Gomes: And, Susan, what's the deadline for responses on that?

Susan Kawaguchi: Let's say Friday.

Chuck Gomes: Friday? Okay. Thanks.

Susan Kawaguchi: Yes.

Chuck Gomes: David, very quickly, I know we're going to continue working on the issue of authoritative, do you have anything you want to add?

David Cake: Not really at this point. I think the discussion is still very fresh and ongoing. I think we may need to redirect that to, I mean, to sort of a freewheeling discussion at the moment and we may need to consider which parts of that definition we actually wish to - or separate out the definition to work out which parts we actually wish to include as requirements, and which parts are more operational. But that's a (unintelligible) for us to consider later. I was just going to say it's very active ongoing interesting discussion at the moment.

Chuck Gomes: And what I'd like to ask you and Mike Palage and Andrew Sullivan to do if the three of you could put your heads together just to see if you can help facilitate - come up with ways to facilitate some sort of closure on this in the coming week, I would appreciate that.

David Cake: We'll certainly try but there's a lot going on.

Chuck Gomes: All I can ask is that you try. So Chuck speaking again. Staff, anything we need to cover before we adjourn? I think we know the action items. Lisa, go ahead - or Marika, go ahead.

Marika Konings: Yes, so thanks, Chuck. This is Marika. We had a question in the chat about the call next week as it happens to coincide with the GDD Summit that may affect some participants. So I don't know if you want to do a check to see who would be unavailable to attend to get an idea about attendance next week. I did note in the chat that it looks like the agenda of the GDD Summit finishes at five o'clock local time while this call would start at six so maybe some

accommodations could be made to find a quiet corner or maybe even a room which would allow working group members to take part in the call.

But again, it's a question that has been put forward so putting it back to you to see how you would like to deal with that.

Chuck Gomes: Well let's plan on having the meeting as scheduled because making changes affects so many people. And if there's some way that we can facilitate cooperation by those in - at the GDD Summit, I'm all supportive of doing that. So - but let's keep it as scheduled because we have too many people in the working group that if we make a change we may benefit three or four and harm seven or eight or more. So let's - thanks for raising that and so again if we can discover anything that'll help cooperation there let's do it.

Lisa.

Lisa Phifer: Thanks, Chuck. I just wanted to briefly recap on our actions that those people that are interested and some kind of newcomers call or tutorial should respond to an online poll that we'll send out. Everyone should be watching for this week's working group poll which will ask follow up questions on the phrasing that we just discussed at length. And everyone on the working group should read the working group rules that were discussed at the beginning of this meeting and will be recirculated on the mailing list. And hopefully we can all try to follow them.

Chuck Gomes: Thanks. Okay. A good meeting. I hope every meeting can be as good as this one. So thanks. Good cooperation, everybody did well .and we have - all have things to follow up on this week so have a good rest of the week at the meeting is adjourned. And the recording can stop.

END