ICANN
Transcription
Next-Gen RDS PDP Working Group Call
Tuesday, 25 April 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-25apr17-en.mp3
Adobe Connect recording: https://participate.icann.org/p49hhqnpgvv/

Attendance of the call is posted on agenda wiki page: https://community.icann.org/x/DcPRAw

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: Great. Thank you again. One moment. Well good morning, good afternoon and evening. Welcome to the GNSO Next Gen RDS PDP Working Group call on 25 April 2017 at 1600 UTC.

In the interest of time today there will be no roll call as we have quite a few participants. Attendance will be taken via the Adobe Connect room so if you are only on the audio bridge would you please let yourself be known now?

Jim Galvin: This is Jim Galvin on the audio bridge.

Michelle DeSmyter: Thank you, Jim. We'll go ahead and know that. And as a reminder…

((Crosstalk))

Daniel Nanghaka: Yes, Daniel here on the audio bridge only. Thank you.

Michelle DeSmyter: Great. Thanks, Daniel.

Mike Hammer: Mike Hammer on the audio bridge.

Michelle DeSmyter: All right thank you, Mike. All right, we will note everyone. And as a reminder to all participants, please state your name before speaking for transcription purposes and also keep your phones and microphones on mute when not speaking to avoid any background noise. With this I will turn the call over to Chuck Gomes.

Chuck Gomes: Thanks, Michelle. And welcome everybody to our call today. Just a quick note on what Michelle asked there a minute ago, what we are asking for is those who are on the audio bridge only and not in Adobe so that we know you can't raise your hand. I think at least one person appears to be in Adobe and on the audio bridge…

Mike Hammer: That would be me, yes.

Chuck Gomes: Okay thanks, Mike. I thought so, so you don't need to let us know if you're in Adobe, it's those who are not in Adobe so that we know you can't raise your hand in Adobe, and we will expect you to speak out. So thanks.

Okay, let's go ahead and get started. We have I think a full agenda today as usual. Let me ask if anyone has a statement of interest update? And for Jim and Daniel certainly if you do just speak up and let us know otherwise raise your hands in Adobe. Okay not seeing or hearing anyone, let's go ahead and go to Agenda Item 2.

And let's quickly get some updates in terms of a couple items that are being worked on behind the scenes, and let's start with Susan and the ccTLD updates.

Susan Kawaguchi: Thanks, Chuck. This is Susan Kawaguchi for the record. We have a list of 13 questions now for ccTLD operators and a growing list of registries we'd like to reach out to. We're trying to find the best contact at those registries to reach out individually to. And so we should have this done this week, I would think, and be ready to do the outreach.

Would it be helpful to send that list of 13 questions out to the full working group at this point for a review?

Chuck Gomes: If they're ready to send out, Susan, I would say go ahead and do that.

Susan Kawaguchi: Okay. We'll - I'll get that out this afternoon. And hopefully we can get some responses in the next few weeks.

Chuck Gomes: Sounds good. Thanks, Susan. Appreciate you leading that effort. And let's go now to David and see where we are at on the definition of authoritative or whatever term we decide to use. David.

David Cake: Yes, so I want to say I'm basically saying we failed to - I think we've decided that not only is there no useful definition of authoritative now but that the term is likely to be confusing enough that perhaps we should just not use it. The - the - basically two issues with the term.

One is confusion of the sort of technical sort of data theoretic sense of authoritative with the legal sense of authoritative, and the other was when we came to look at a technical definition of authoritative we found that the - that while it is precisely - well while it is definitely defined all uses of the term within normal sort of IETF use, refers specifically to the DNS, and the definitions for its use within the DNS were not only not useful being too specific to the DNS, but were probably kind of actively misleading due to some quirks of the way the DNS uses the term.

Rather than try to adapt those definitions to - to distract the sense we're using, I guess the sense is that perhaps we should just avoid the term authoritative for clarity and try and find a sort of equivalent wording. My feeling is that - we don't seem to have found anyone to volunteer or reached consensus on equivalent wording. And my feeling is that we should sort of kick that back to the main working group anyway because at that point the clearing up the very specific issues that we formed the small group for no longer really applies.

So essentially we're going to say we failed to find a useful definition. We think there are very good reasons why it is confusing. Perhaps we'll - we're just going to kick that - the wording question back to the main group. I will write a message to the group going into some more detail about exactly why it's not so helpful. And thank you all.

Chuck Gomes: David, this is Chuck. Let me ask you, so the three of you are recommending that we avoid the - using the term "authoritative." Now is it my understanding that you're going to suggest an alternative term where we might previously have been using authoritative? Is that correct?

David Cake: I don't think we've come up with that. And I really think at that - I think we can explain what we mean by the term and sort of throw it back to the main group for any suggestions about final wording. I don't - like I don't think the reasons why we picked that small group - we should - I think the reasons why we had that small group are now over and we should - for future wording everyone should have a say in it. But I will suggest some alternate wording.

Chuck Gomes: Okay thank you. Appreciate that. Any questions or comments on that? Note that Lisa says we still need a definition for a term to reflect the concept that the working group was trying to reflect in the purpose statement. David, do you want to comment on that?

David Cake: Yes, I do think we can - I do think we have narrowed down what sense the working group was reaching for in the purpose statement which is to isolate that, basically that (unintelligible) extent. So what we're trying to get at is able to access the original source of data. So - you know, the original repository of data within the system. I've got to get the wording exactly right, but it is that database theoretic sense and we're - we think the system is intending to use it.

Now there are oddities of how that works within the DNS, because DNS - the DNS system has, you know, primary and secondary name servers both of which are authoritative. But - and the definitions within DNS reflect that so that just sort of becomes unnecessarily confusing.

But that's the thing we are getting at is that when we mean authoritative, we mean that there is, you know, a place within the system that is - the repository of the data and that we are able to access it directly rather than the data entirely being cached or the issue - part of what - the discussion that we had in Copenhagen was actually trying to in some cases avoid committing the system - we sort of wanted to indicate the access to authoritative data was a goal but not always a requirement.

It was a requirement that it happened but we didn't want to constrain, you know, wanted to make it clear that that was a requirement of the system, but it has a repository of data that was understood, a single repository of data that is understood to be the one sort of source, but we didn't want to jump ahead ourselves and make requirements that would preclude some design decisions in Phase 2. So it's - why exactly where we're using the term gets a little (unintelligible).

But again, I'm saying I think this is a discussion that the whole group needs to be concerned with, so…

Chuck Gomes: Okay but…

((Crosstalk))

Chuck Gomes: …you're going to send detail in writing to the list, correct?

David Cake: Yes I am.

Chuck Gomes: Okay. And then Andrew, please join in that - I see your chat, sorry about the AC problems. But, yes, please feel free to suggest some - a few different formulations as well. So that would be fine. And of course if Mike Palage, one of the three of you that worked on this wants to jump in anytime - he doesn't appear to be on the call today he's welcome to as well. And we'll discuss it as an entire group. So if that could be done this week that would be great. Thank you very much. Any questions?

Okay, all right let's then move ahead to Agenda Item 3 and the change in our work plan that the leadership team put out to the group. I think the message went out on Saturday, at least the one with the attachment that I forgot the first time.

And we are going to let Lisa go over that and then entertain any questions that anyone has. So Lisa, if you can bring up that - those two slides and then go over them to show people how we are changing course a little bit in terms of our work plan, overall work plan of course and the charter stays the same. But our order of events will change a little bit. So, Lisa, it's all yours.

Lisa Phifer: Thanks, Chuck. And this is Lisa Phifer for the record. And I'm going to keep the control of the slides just for a moment and then I will take the sync off so that you can all step back and forth between them. But I want to address the slide that's on the screen for the moment.

So the first slide in this little three slide deck, you have seen before. This is actually the approach to reaching consensus in Phase 1 that we originally

discussed at our meeting in Hyderabad and is still the track that we are following where we are deliberating on the five fundamental questions to try to provide a recommended answer to that foundational question of whether the existing Whois system can be tweaked to meet the fundamental requirements, or we need a next-generation system in order to do that.

All of this working group's agreements and recommendations regarding those fundamental questions as well as the answer to that big foundational question would be part of our first initial report which is the first point at which we go for formal public comment. That doesn't mean that we can't seek informal input between now and then. Having done that and received public comments back and factored them into our work then we would step through the rest of the questions in our charter that has to do with looking at factors such as cost, risk and benefits through the lens of which system this working group is recommending, that is a new one or tweaks to existing Whois.

And the whole idea is that we'd move towards actual formal consensus as we go through this series of the first, second and then of course our final report for Phase 1 remembering that we have in this PDP, three phases. After we exit Phase 1, if this working group recommends that a next generation system be developed, and the - that recommendation goes to Council and we decide to move forward on defining a next generation system, only then would we go to Phase 2 where we have to hammer out in detail policies for a next gen system as well as implementation guidance and coexistence guidance. But that's not shown on this slide.

So with that as the context, let me go to the second page. This is the task that we've been embroiled in for quite a while now. We have been looking at the first three charter questions and as those of you that have been part of all of this since last fall recall, we kind of switched gears sometime last fall, I think early December, and started looking at key concepts for those first three charter questions of use or purpose, users and purposes, data elements and then privacy and data protection.

And that's what we've been doing in our meetings since then is looking at key concepts and iterating or bouncing between these three areas, the three charter questions. The change in - that the leadership team concluded was necessary after our last call was that we actually step forward from looking at only those three questions and look at the question of access, again keeping our focus on thin data for now.

The reason that we thought this change might be useful is that in our deliberations on uses and purposes, data elements and privacy, and if you think back to last week's call in particular we were looking at data elements and the purposes for each data element. And we keep on hitting a stumbling block that some people feel that they can't answer those questions that are posed or agree to potential key concepts in those areas unless they know whether access will remain entirely public or whether there will be some kind of filtered, tiered, gated, however you want to - whatever term you want to apply to it but some kinds of control to access to data elements.

So what the leadership team decided might be helpful to make us be able to reach better agreement on those first three questions was actually to go ahead and let us focus for a moment on access again still looking only at thin data but look at access and try to answer that question and see if we can reach some agreement there that would allow us to then return to looking at users, purposes, data elements and privacy given that agreement on whether access would remain entirely public or not.

So as this entire process is iterative, we are not just leaving the three - first three questions as they are today but we will return to them. And then once we reach some level of consensus, rough consensus, on that we would move forward into looking at thick data in Task 12C.

And the slide here depicts that we have a first and second pass defined in our work plan. In the second pass, we would go back and look at these initial key

concepts that we've been developing and will continue to develop, and try to make sure that they are framed as requirements to answer those fundamental - the five fundamental questions, to answer the foundational question.

And you probably recall from a previous meeting that we said as a target that we would try to start at least preparation of that first initial report by ICANN 60 this fall in Abu Dhabi.

So now I will move to the third slide, and I'm going to take synchronization off in case you wish to scroll through the deck yourself. The third slide actually lays out some target dates for all of those steps in order to get us from where we are today, deliberating on the first three questions in Task 12A, moving us through the summer so that by the time that we meet in Johannesburg at ICANN 59, possibly we could be ready to start looking at key concepts for access to thick data. We believe that I would be very effective use of our face-to-face meeting since we think that will be a really challenging question for us to try to address.

And then use the summer for our second pass, going through the key concepts that we develop thus far and try to harden them into some draft requirements that would allow us to begin deliberating on that foundational question in advance of our ICANN 60 meeting. So that's the rough timeline that we came out with in order to try to get us to the place where we're ready to at least draft that first initial report by the time that we get to ICANN 60.

And I'll turn it back to you now, Chuck.

Chuck Gomes: Thanks, Lisa. And I'm going to open it up for questions. Before it do that, let me point out then that we would move to Step 12B after we finish discussing this change today. So in our meeting today we would start working on the gated access questions. So please be aware of that. Now let me open it up for any questions or comments. Marc, go ahead.

Marc Anderson: Thanks, Chuck. It's Marc Anderson. You know, first let me, you know, give my appreciation to the leadership team for all the time and thought they put into this. You know, I do agree that, you know, we keep stumbling on, you know, this problem of, you know, collection without talking about access, and that does seem to be a stumbling point. But I can't help thinking that we're going to run into the same problem with thin versus thick.

You know, and I'm, you know, I'm not sure, you know, I'm advocating for or, you know, one way or the other but, you know, I'm concerned that constraining ourselves to thin data - only thin data now we're going to run into the same problem we ran into before with collection versus access only.

You know, so again, you know, I think the approach is, you know, the approach of talking about access now makes sense. I'm just, you know, not sure it makes sense to tackle just thin data now. Thank you.

Chuck Gomes: Thanks, Marc. It's Chuck. And you may be right. We actually talked about that a little bit as a leadership team. And the approach we decided was if we find that that happens we can expand the thick data sooner. So let's see how it goes. And if we see that we're stumbling because of that, we can adjust, but thanks for the comments. Theo, your turn.

Theo Geurts: Thanks, Chuck. I'm sort of disagreeing with Marc here. Some good suggestions there, still though. But I think the approach is pretty good. Let's use the approach for thin data, see where we go from there, and get some more insight on the whole gated stuff. I think that's where most of us are struggling. The further we get ahead on the gated access stuff the more you get a whole picture of where everything is going to fit there and it's going to be like a personal, nearing some phase of completion there.

And I think it will be easier to - for the people on the working group to comprehend which goes where and how eventually it might be - going to look

like and when it comes to the question of thin data or thick data I think that's a matter of where it's going to be stored eventually and that is a different discussion so I'm not too worried about that. So I think let's use this approach, see how far we get. Thanks.

Chuck Gomes: Thanks, Theo. And I don't know if Lisa - this is Chuck - I don't know if Lisa or I pointed out - I think I did in the message that I sent out on Saturday, but the leadership team just didn't come up with this on their own; it was actually in response to quite a few comments from a lot of people over the last several weeks both in meeting chat as well as in email and in verbal comments in our meetings the last few weeks.

So we felt like this was a lot of you were commenting to - about this hurdle we keep running into instead of jumping over. So it is thanks to the input from lots of you that we went this direction. Nathalie, it's your turn.

Nathalie Coupet: Can you hear me?

Chuck Gomes: Yes.

Nathalie Coupet: Okay. I was - as an end user I must say I'm quite sensitive to both sides, and I have concern about privacy and also concerns about - I want cyber security sector to be able to do its job properly. As an end user I'm also aware of the growing threats that we're facing today and I don't think I would be happy to have my privacy secured knowing that all these criminals are loose. So I want to make sure that Allison's concerns are properly addressed. I feel that we - she says the same thing every time and we never really deal with what she's saying.

And I think it's, as far as I'm concerned, this is crucial. I would like to understand how we can accommodate her concerns, let her do her job as best as she can and still protect privacy. And I think we might need to add another step, like a meta process. What are the rules to - so that we should

apply in order to further this conversation and go into negotiations really because we will be sacrificing somebody's concerns, well part of it I hope, not all of it. And I want to make sure that we have clear rules as to what we can do, what we cannot do when we can sacrifice something in favor of something else because they may be equally important. But I feel we haven't talked about this.

And I'm - I like rules, I like - I want to understand the process. And I feel that we need to discuss about a meta process. Is there a pendulum maybe within this - these overarching concerns of trying to accommodate both privacy and cyber security concerns? Is there a pendulum that swings in more or less in the privacy direction and then goes back to security concerns?

But is there something like that going on? And if not, I mean, I just want to understand I would like to have a meta process so that we can really have a negotiation and not, at some point, arrive to the conclusion that we need to exclude someone. And if we do need to exclude someone at least we know why and this is approved because I think that's also the biggest hurdle is that we all know nothing - we can't all have our way. But we don't talk about this. So what can we do and what can't we do? What are we willing to sacrifice and what are we willing to keep and how? That's my biggest concern.

Chuck Gomes: Thanks, Nathalie. This is Chuck. And I'm going to come back to you because I need to better understand what you're thinking of in terms of a meta process. You're absolutely right that we need to justify whatever decisions we make. If we make a decision to go one direction and not another, we're going to need to base that on objective information. Now that objective information may be laws, in some jurisdictions. It may be need, a legitimate need that particular interests have whether it be for privacy or for access and so on.

So can you help me understand maybe with an example - I don't know if an example really is possible - of what you're thinking of in terms of a meta process? I think I'm in full agreement with you that we need to base whatever

decisions we make on objective data, and clear decisions knowing the tradeoffs. But can you help me better understand what you mean by a meta process?

Nathalie Coupet: The framework of discussion, how negotiation as opposed to go on the rules the rules of the game. When you play a game you always have the rules beforehand. And you know exactly what you can and cannot do. And this prevents us from stalling at some point and people may be - do not want to get into fights with other people because - I mean, we need to establish a framework for these negotiations because that's what it is, it's a negotiation. So I feel that we're missing the rules of engagement.

Chuck Gomes: Okay.

Nathalie Coupet: That's what I mean.

Chuck Gomes: Thank you. Now we do have rules of engagement in our charter so I certainly encourage you to go back and look at those including how to deal with differences of opinion and so forth. So we do have that framework that's pretty well laid out. Whether that's all that you're talking about, I'm not sure. But let's listen to some others. Andrew, go ahead.

Andrew Sullivan: Let's see if Adobe Connect likes this. I…

Chuck Gomes: You're coming through a little lightly, Andrew.

Andrew Sullivan: Now let's see if this is any better?

Chuck Gomes: That is.

Andrew Sullivan: Okay good. I said in the chat that I disagreed strongly about the thick versus thin remark that was made earlier. And I just, rather than trying to type it I thought I would explain why. When you look at a given data element, what

you want to know is why it's collected. And of course why it's collected is partly bound up with, you know, what do you want to do with it later. And so the objections that people have been making that they can't answer the question about whether a data point should be collected or by whom, because they don't know it's going to be used later, is a legitimate one in that it's part of the reasons why you collect it.

But the thick versus thin discussion is actually about which data elements we collect and who gets to see them. And so it's possible for us to have a generic discussion about whether there is gated access and what it would look like before we tackle the problem of which data elements precisely we're going to collect. And I think the reason to handle the thin ones all in one go at the beginning here is because we seem to have at least from my point of view, we seem to have converged on the idea that almost all of the stuff that we've been talking about is thin, maybe all of the stuff but if not all of it then almost all of it, is necessary for the functioning of the system at all.

And if any of them don't work, if any of them aren't allowed to be collected then in fact we don't have a system and we can all go home. So I think that this is a legitimate distinction to make and also I think that it's the right way to go. So I approve of this step. But that's the reason that I think the thick versus thin discussion can be saved until later. Thanks.

Chuck Gomes: Thanks, Andrew. This is Chuck again. Mike, go ahead.

Michael Hammer: Thank you. This is Michael Hammer. I'm going to state something that may sound a bit aggressive to some folks but I hope that it provokes some deep thinking. I'm a security and anti-abuse guy, and there have been discussions of a day without security. And I'd like people to think about the implications. It's already difficult enough to fight abuse and in many quarters there's a sense that we're losing the battle.

So to the extent that folks aggressively pursue the privacy perspective through either not having information or gating it, it may make folks in the security and anti-abuse community really question what are they doing? Why are they fighting this fight because for many of us, it's not simply about money. And that's all I have to say.

Chuck Gomes: So, Michael, this is Chuck. I have a question for you, would you agree with me that in various jurisdictions around the world, there are laws, regulations, that require privacy of data and protection of data?

Michael Hammer: Oh, I absolutely get that, but I also understand that when things hit the fan, many of the same people who are advocating these laws are the first ones to say, "make the pain go away." They want their cake and they want to eat it too.

Chuck Gomes: So I - this is Chuck again. I doubt that there's anybody in our group - I'd like to think there's no one in our group that doesn't strongly advocate for security. So I think we're on the same page there, all of us I hope. But we do run into conflicts. And what our task is, is to see how we deal with those conflicts and provide the best security possible while at the same time allowing people from different jurisdictions to comply with local laws. So that's what we have to do.

Michael Hammer: So I'll jump in with another point, which is it's quite easy, well, I won't say quite easy, but, you know, one of the solutions is to drop route when there's abuse. And I'm speaking as somebody who in extreme circumstances have cut off entire countries and not just ones that don't really have access. So, you know, to the extent that jurisdictions put privacy ahead of security, they may find that the people that they're protecting the privacy of, may not get access to resources.

Chuck Gomes: And of course that's why we're getting into gated access right now. So let me jump ahead to Theo.

Theo Geurts: Thanks, Chuck. You know, to - in response to the previous speaker, there is nobody against or in favor that abuse levels should rise. There's nobody who wants to have child abuse, I mean, we're all against it. And I'm speaking as a registrar. But as a registrar, I'm looking at this from a business perspective also, there's abuse, and I'm dealing with a lot of new regulations coming through the new GDPR. I mean, the fines are insane.

Is there going to be enforcement? Yes, there is going to be enforcement. That enforcement we didn't have the enforcement for the last 10 years, and that is exactly the point that is where we got a sort of a free ride here when it comes to the Whois as it is now, I mean, there was no enforcement. So we got very lucky there as registrars, we didn't go - we went not under the bus but we're going to be under the bus in 2018.

So this is critical for us because if we're all going out of business, and this is not just a problem that is affecting Europe, it is affecting every registrar and registry on this globe who wants to deal with European customers. Now, we could come up with scenarios where we don't serve those regions in Europe anymore as a registrar, but that would be insane. That is not economical not feasible and it is not within the mission of ICANN. It's a global thing, the Internet. So we've got to keep that in mind.

And if you look at complying with the law, this is not something new. We've done it in China last year. I mean, there were a whole bunch of regulations that were being imposed on Chinese registrars, Chinese registries and the registries outside of China. Did we do - regarding compliance with the law. It's going to be easy? No, it's not easy but it's something we must do. And this is something only regulations are being imposed on us and we need to do something with it.

And again, we are not against abuse, we are not - we want to make sure that there is no abuse but something has to give here so let's explore gated

access because we need to do something here. And I think we are all on the same page as everybody - as Chuck just mentioned. Thanks.

Chuck Gomes: Thanks, Theo. Chuck again. David, go ahead.

David Cake: Yes, I mean, I just want to make the point, I mean, all of us understand that there is a trade-off between - it's not a direct opposition, but there are some, you know, awkward trade-offs between privacy and security. So in one direction sometimes, you know, there are ways in which we define security where having your information (unintelligible) public reduces it.

But the main point I want to make is there is a lot of, I mean, the argument about is there - is there going to be privacy regulations has already been made outside this group. It has to change, we have to accommodate it. We have to make a system that is legal for Europe and other countries with strong data protection law. We can't avoid it. The decision has been made outside of this group.

So any argument that says well, those laws are bad, we should just ignore them, is not or otherwise says that, you know, the privacy arguments being made here are wrong because, you know, they may have security consequences - the arguments have been made, we have to - that is part of the purpose of this group is to make something that lives with current law. Certainly people are - some people have said, you know, able to advocate for - to have the law changed and I wish them well in that endeavor.

Certainly some people are - may decide that complying with some European law may be problematic for them and well, you know, they're just going to have - not operate in some jurisdictions. But the bulk of the - I think realize that we literally have no choice but to try and comply with the law as it exists, that is going to have some consequences in the way people do their business. And we now need to work on ways that we can, accommodate it.

Just arguing that the intent of having better privacy protection is problematic is not helpful.

That argument has been made well outside of ICANN at the, you know, European parliamentary level and so forth, and in many local jurisdictions. I don't see that arguing against the, you know, laws - its compliance with laws that of already been made essentially serves any useful value to this specific group, which already has a lot to deal with in, you know, just understanding what those laws are and how it affects us. And of course we should have a flexible system that does not assume that the same laws apply to every jurisdiction.

It's understood but some of these arguments seem to be saying well, the European laws are bad; we should, you know, data protection law is bad. Maybe, but complying with them is what we're here to do. I don't really - I find some of these arguments distracting at best. Thank you.

Chuck Gomes: Thanks, David. And I'm going to - we're going to move onto the next agenda item now but I want to let you know that going forward I'm going to try to get us beyond these high theoretical levels, like we've been talking for the last 15, 20 minutes, and force us into very specific questions that we need to find answers to.

I'm also going to be more assertive when we come across terms that we can spend weeks on. We're going to eventually have to get the terms right and I think we can. But I'm going to try to for us to look at very specific questions in our charter and to help us come to answers to the questions we have in our charter to answer.

So you may find me cutting some discussions off and maybe postponing them until later, unless they're just absolutely essential and we can't make any progress. But if all of you will think back over the last several weeks,

we've spent an awful lot of time and not come up with very many answers. And we need to start coming up with answers.

Now, we're going to need practical examples, we're going to need situations illustrated so that we know what kind of things we need to deal with. And we have to do what Nathalie said and we're going to have to make some hard decisions based on the information that we come across.

So if I'm a little less tolerant in the next few weeks and months in terms of allowing some discussions to go on and on and people expressing their opinions and so forth, you know, most of us have done a pretty good job so far of communicating our positions and so forth. Now we need to get down and work together collaboratively to figure out where we're going to go and what answers we're going to come up with for the questions that we have to ask.

So let me let Paul talk and then we're going to go to the next agenda item.

Paul Keating: Hi. This is Paul Keating for the record. I have - I apologize very much, I like very much what you just said, and I'm new to the group so please don't throw too many cannon shells my way. But it seems to me that we're having what we lawyers would say is a jurisdictional discussion here. There's a lot of messages in the chat that I have read, there are a lot of statements that I've heard that seem to prescribe that just because the European community, of which I'm a member, where I live, has dictated a set of rules that the whole world has to jump up and down and comply.

And we need to remember that laws are jurisdictional, and our problem that we're dealing is we're dealing with a global beast called the Internet in a jurisdictional world which is inherently national. And so one country can claim that its laws are going to be sacrosanct above all others, and another country can claim the same thing. But these are nothing but the same issues that are - that everyone's forefathers fought about 300, 400, 500 years ago.

We need to get a - we need to come to grips with whether we're going to do two things, one of two things. We are going to either create a system that is going to comply globally all of the rules and regulations that we know of, or we're going to create a system that complies with what we think should be the rules and regulations of the Whois, okay?

As to the former, I think unfortunately I think it's an impossible decision for two reasons. One is, we don't have the capacity as a working group to understand what the global - what the rules are going to be in every jurisdiction that the Internet is going to come across. And, Number 2 is, all of those rules may change tomorrow. Okay? So that's very difficult to plan for that global consistency.

What we could do is create our own rules of what generally we think the Whois system should be and why as guiding principles. Now, with that regard, we have several problems, one of which I've heard is, oh, gee whiz, I'm a registrar in Austria and I can't possibly comply with the Austrian obligations of privacy for my clients. Okay, so my first response is, you can move from Austria. You don't have to be in Austria, you can be a registrar, you can physically locate your company in Aruba. Austria would have no control over you whatsoever, okay?

So in other words, we need to either - we need to plan what we can plan. We can't - we can't plan for everything. And although I understand the need for privacy and the conflict with security, there is a certain amount of practicality that we have to approach the problem with. We have to say to ourselves, okay, you want to register a domain name, you either need to put your information down on the Whois or you have to have some else's information down on the Whois who will verify your credentials and protect your privacy. But I don't see any other alternative to what we're doing. Thank you.

Chuck Gomes: Thank you, Paul. Now we're moving to agenda item 4, because we could talk at these high levels forever and not get anywhere. Charter Sub Question 5.1 is, "Should gTLD registration thin data be entirely public or should access be controlled?" And if you express an opinion I would ask you to briefly fight the rationale for your opinion on this, okay? So the question is, "Should gTLD registration thin data be entirely public or should access be controlled?"

And if you're raising your hand I'm assuming you're going to respond to that question. And provide your justification. But please be brief, we have 29 people on this call plus some additional staff members. And we want to give as many people a chance to speak as possible. So David, is your hand still up to answer that question? Okay. Paul, are you going to answer that question, give your opinion?

Paul Keating: Love to. Love to. It must be public just as any other registry of ownership information must be public, in my opinion. We need to understand who is the ultimate beneficial owner and who is the ultimate responsible party who owns property. Okay? There are justifiable reasons for remaining private and protecting your privacy. I understand them. I get them as a lawyer all the time. But there are means of protecting that privacy which do not equate to taking the entirety of the Whois record offline from a public standpoint or placing it behind a wall garden which is what we're really talking about in terms of gated. Thank you.

Chuck Gomes: So, Paul, you believe that all the thin data elements that we've been focusing on should remain public and that privacy - any privacy that's needed can be handled through other means rather than hiding those details from public access, is that correct?

Paul Keating: Correct. In other words, you can have a qualified party who is serving the role of being the public front person for the record, but who knows of your credibility and knows your credentials and can essentially vouch for you for the purposes of maintaining the security aspects of the Whois.

Chuck Gomes: Okay, you're jumping into thick data, okay?

Paul Keating: Sorry, but I believe…

((Crosstalk))

Chuck Gomes: …talking about right now is thin data. There's no…

Paul Keating: Okay, but I believe that thin data should apply to the thick data so I'm - I believe that there's…

((Crosstalk))

Chuck Gomes: Stay with our task, please.

Paul Keating: I'm sorry, I'm trying. I'm trying.

Chuck Gomes: Okay. So let's stick to thin data right now. Okay?

Paul Keating: Correct, okay.

Chuck Gomes: Okay, and your position is clear, okay?

Paul Keating: Thank you.

Chuck Gomes: Jim, go ahead. Jim, we're not hearing you. I don't know if you're on mute. Jim Galvin. Still not hearing anything. While we're waiting here, I'm about to do a quick little live meeting poll so prepare yourself to use Adobe if you're in Adobe; those that aren't we'll give you other ways to speak up. But I just want to call attention to the fact that just before our meeting today Vicky Scheckler chimed in and she also believes that all the thin data elements should be -

should remain publicly available so that's just - I'm just throwing that in while we're waiting for other people to jump in.

And since nobody is - has their hand up, how many of you…

Marina Lewis: Excuse me, Chuck?

Chuck Gomes: Excuse me?

Marina Lewis: Hi. Hi, Chuck. I'm sorry, this is Marina Lewis, I'm on the audio bridge only and I was actually going to see if I could pipe in…

Chuck Gomes: Oh okay. Go ahead, Marina. Speak up.

Marina Lewis: Okay.

Chuck Gomes: Thanks for speaking up.

Marina Lewis: Yes, sorry. Thanks, Chuck. Real quick I'll just say I am proponent of having the thin data remain public. And the reason I say that is because I do draw a distinction, and I realize that we are getting into some fundamental kind of high level stuff so I'll keep that to a minimum, but perhaps this goes to Nathalie's comment earlier about sort of rules or principles. My overarching approach to this is that I draw a distinction between those who register domain names and they create websites versus those who are true end users who visit websites. I am a very, very strong advocate for privacy concerns for people who use the Internet, for people who use emails and visit websites.

However, I agree with Paul in this case that if you are essentially a Website operator or you are a mail serve operator, domain name registrant, I believe you are more than just a user at that point; you are a creator of the Internet and the domain name system, and as a result of that, you have an obligation, like Paul said, to make your contact information known, the same way you

would any other participant or link in any type of infrastructure, say real property, or any other type of asset that the public uses.

I mean, we forget that this - the Internet is by definition a public framework. And so I believe that if you are going to be part and parcel of that framework, your information needs to be as public as anybody else's. So that's my approach. Thanks, Chuck.

Chuck Gomes: Thanks, Marina. So we have three people I think agreeing so far, and if we include Vicky's pre-meeting input. Andrew, you're next.

Andrew Sullivan: Hi there. Yes, so I just…

Chuck Gomes: A little weak again, Andrew.

((Crosstalk))

Andrew Sullivan: I'm chiming in - is this any better?

Chuck Gomes: Yes, that's better.

Andrew Sullivan: All right, I'm chiming in again because I'm a little bit nervous about this distinction between like the real end users and other people. You know, that - the Internet is designed as an end to end system where we don't make a lot of distinctions between the kinds of participation of various participants. And what that really does is change the rules so there is, you know, you must be this tall to ride rule.

So I'm anxious that we not - that we not assume pieces of the architecture that are basically just the way the World Wide Web works today. That is not how the architecture is really supposed to work. And it so happens that it's emerged that way for the time being, but there's no reason to suppose that that's a long term fact.

For instance, imagine that the Internet - the so called Internet of Things world starts using domain names ubiquitously in order to identify things inside your house. Suddenly we'd have a real problem with personally identifying information on these domain names that are supposed to be just, you know, we designed a policy for people who are running websites and so on. I don't really want people - everybody in the world - to be able to look up my name and address just because I've registered my thermostat on the Internet.

So that seems to me to be something that is a little bit dangerous. And we need not to be making those kinds of distinctions. Now all of this, is nevertheless, about thick data, and I think that that's the point that we were starting with before. So I think that the thin data questions are very, very limited in the kinds of data that we're talking about and I think that we can continue to talk about those things precisely because they're not personally identifiable information - or identifying rather. Thank you.

Chuck Gomes: Thanks, Andrew. And of course we're coming back to what Marc Anderson's concern earlier, it's tough for us to just talk about thin data. Most of the - many of the comments that have been made by the last several speakers have merged into the thick data issue and I think that's the concern Marc had. But for now we're going to focus on the thin data.

So I'm going to ask a question of all of you now, I'll ask the question and I'll let Paul speak before I ask for the responses. But the question I'm going to ask is this, I would like any of you on the call, and if you're not in Adobe I'll ask you to speak up when we get to that point, to - if you think that any of the thin data elements, notice I said "thin" - and we've defined that - should not be public, so I'm going to ask you in a little bit to put a red X in there. Don't do it yet. If you think that there's some thin elements that should not be public, okay? And of course I'm going to ask you to explain why so be prepared to do that.

Now, Paul, go ahead.

((Crosstalk))

Paul Keating: Please remind me what is (unintelligible)…

Chuck Gomes: You're not coming - I can't understand you, I don't know what's - there's some interference. Try it again.

Paul Keating: I apologize, can you hear me?

Chuck Gomes: Yes, I think so.

Paul Keating: Okay. So the question is (unintelligible) and anyone else who doesn't remember, but what is the definition that you're using generally (unintelligible) data?

Chuck Gomes: Okay, I'll ask staff to put that definition up on - in Adobe. And in the meantime, Marc Anderson, go ahead.

Marc Anderson: Thanks, Chuck. It's Marc Anderson. I want to clarify, I guess are we equating gated access with saying that the data is not publicly available? Because if so, I'm not sure I agree with that. You know, and I'm looking for I think somebody stated in chat earlier that, you know, they, you know, they agree that it should be public but there should be some controls on it.

And, you know, I think I agree with that statement and, you know, I think there's some disagreement or some feeling that gated access means it's no longer public. And, you know, I don't agree with that. I think you can have gated access, you can have controls on the data, but still have the data public.

So I guess if you ask the question in the way you've worded it now I'm going to have trouble answering it. Thank you.

Chuck Gomes: Okay. You confused me, Marc. The - I believe what people mean by public is it's anybody can see it. Is that not clear?

Marc Anderson: Well so if I say - if I, you know, so you have the question, if you think that any thin data elements should not be made public, you know, put a…

((Crosstalk))

Chuck Gomes: In other words, shouldn't be displayed the way they are today.

Marc Anderson: All right so if I - does that mean I agree or disagree with gated access for thin data?

Chuck Gomes: Well, we'll get to the - you don't need gated access if something's publicly available. That make sense?

Marc Anderson: Yes and no because I'm not sure I agree with that. So there's some data that you, for instance, some data is available in DNS, for instance, name servers. Right? So, you know, you can access some…

((Crosstalk))

Chuck Gomes: Okay let me - I'm going to cut you off because I want to be more specific. We're talking about the RDS, okay? So - and so the issue is are there any thin data elements, okay, should not be publicly displayed as they are today in Whois in a new RDS system?

((Crosstalk))

Marc Anderson: Okay.

Chuck Gomes: Is that clear?

Marc Anderson: It is.

Chuck Gomes: Okay, now whether they're available somewhere else or not, what we're talking about is the RDS right now. Okay? Is that - is my question clearer?

Paul Keating: Did they send a new one? Okay, so I understand that you sent the…

((Crosstalk))

Chuck Gomes: I'm hearing somebody in the - it sounds like in the background. Is that you, Paul? I'm trying to - I don't know where that was coming from. It sounded like in an echo chamber. So now Paul, have you - you can scroll on here for the thin data elements - Lisa, help me out here, where on the screen are the - in fact, why don't you take control of the scrolling and show the list of thin data elements so that there's a very clear definition of what we're talking about.

Lisa Phifer: Chuck, the document that I'm displaying there on the screen says in December 2016 the working group agreed to focus its deliberation on thin data as defined by the Whois report. Apologies, I just scrolled away.

Chuck Gomes: Yes, I was looking at what you were reading and then it disappeared. Okay, so in that middle paragraph there, right? Just above 2.1.2?

Lisa Phifer: Right. So the data set for thin data today includes the sponsoring registrar, status of the registration, creation and expiration dates, name server data, the last time the record was updated, and a link to the registrar's Whois service, it also includes the domain name itself. And I believe that someone copied a Whois record into chat as well.

Chuck Gomes: See I'm way off in the chat. I haven't been - I was up too high. So…

Lisa Phifer: There you go. It's Chris Pelling…

((Crosstalk))

Chuck Gomes: That's what we're talking about - those elements are what we're talking about for thin data. Okay? Andrew, go ahead.

Andrew Sullivan: Hi there. This is Andrew Sullivan again. So I think in this conversation we're conflating a couple of things and it's important for us to make the distinction. The current Whois model is both it publishes a large amount of data, and that's the thick thin distinction. And the other thing about it is that it has completely anonymous on authenticated access.

So, you know, if a Whois server is listening on Port 43, it just replies to whatever query it gets. Gated access is about two things, it is about whether you reply at all to a given query and whether you reply with a given data element. It has both of those qualities because what it does is it authenticates the user and then it says you may, you know, these are the things that such a user is allowed to retrieve.

And if the user attempts to retrieve things beyond that then it just doesn't get them, but also if the user, for instance, attempts to retrieve more quickly than the user is supposed to retrieve, then that user will be limited in some way like perhaps it won't get an answer or it will get an error message or whatever. And both of these are elements of gated access. And we actually have this kind of gated access today in the Whois, most of the large gTLDs at least, have a contractual provision that allows them to rate limit Whois access.

And that rate limiting is effectively using the IP address of the source query as an authentication token and it will only give you an answer so often within a given minute. That is - that's a kind of gated access, and we've already got

it today. So I want people to understand that this is not actually an innovation, it's just an innovation that allows us to do gated access in a more sophisticated and in my opinion, rather more reasonable way. Thanks.

Chuck Gomes: Thanks, Andrew. Alex, go ahead.

Alex Deacon: Thank you, Chuck. This is Alex. Yes, so I don't disagree with Andrew there, but I think for the purposes of our conversation and for future deliberations, I think it will be helpful if we separate the concepts of gated access, which I see indicated and authorized access to data or some subset of data and the more technical, you know, aspects of running Internet services around rate limiting and the like. I think if we talk about them together as kind of one concept it may complicate future debates. So I think both concepts are important and we need to ensure that we take, you know, rate limiting and other, you know, services into effect. But if we separate them I think it'll make our lives easier moving forward.

Chuck Gomes: Thanks, Alex. I think you're right. And not detracting at all with the distinction that - or the two examples of gated access that Andrew gave. What we're really focusing on now, and let's keep it fairly narrow, okay, are there any of the thin data elements, and I'd like you - if you think there's one or more of the thin data elements that should not be made publicly available, and that could happen through a rate limited display, the point is there's really no restriction on somebody getting that data other than business management things like rate limiting and things like that.

So is there - does anyone on this call - if you think that there are any thin data elements that should not be made publicly access in the RDS, put a red X in the Adobe or if you're not in Adobe please speak up and tell me who you are so I can get that. Any red Xs? Let me scroll down so I can see. Because I'm going to draw a conclusion from what I see or don't see here. Okay, Marc Anderson, go ahead. You need to explain yourself. Which data elements do you think should not be publicly displayed? And why?

Marc Anderson: Thanks, Chuck. It's Marc Anderson. You know, I think, you know, I'm having a little bit of trouble with the question. And, you know, as you noticed earlier, but, you know, I'm not sure, you know, you know, I'm not sure that unlimited anonymous public access to, you know, the Whois server, the referral URL, updated date, creation date and expiration date are all necessary.

And, you know, I'm trying to apply what we learned from data commissioners, you know, earlier and that, you know, collecting data, you need to have a legitimate purpose for that. And I'm not sure what that is. And, you know, you're looking at the status information, some of that may not even be applicable for an unlimited public access model. So I'm not sure, you know, I think…

((Crosstalk))

Chuck Gomes: Marc, you don't think that we can find a legitimate purpose for each one of those elements?

Marc Anderson: No, I stated - I think you can find - you can come up with a legitimate purpose for an awful lot of things. Is that necessary for the operation of an RDS system? Is it applicable with - or does it comply with applicable law? You know, I think, you know, those things have to be answered as well. It's not just can you come up with a possible purpose for this data element. I think I could come up with a possible purpose for any data element.

Chuck Gomes: Do you think that displaying any of these thin data elements breaks any laws?

Marc Anderson: I didn't - I didn't say that. You know, and that wasn't the question, you know, the question was are any of these elements - any of these thin data elements ones that should not be publicly displayed.

Chuck Gomes: I was following up what you said, you're the one that brought up the laws.

Marc Anderson: Okay, I'm not sure - I'm not sure exactly what you're asking at this point then, Chuck.

Chuck Gomes: Well, you see, we're getting into - we can get so fine in terms of every little minute detail that we will never accomplish anything. Most of the people on the call seem to believe that there's not a problem with displaying these thin data elements publicly. Okay, so that anybody understanding that whoever is displaying this data will have certain things like rate limiters and things like that. You seem to - so far you're the only one that seems to be - you and Theo so I'll let Theo speak too - think that there's a problem with displaying any - some of these elements publicly.

So I'm just trying to press that and understand it better. I'll come back to you, Marc. Let you think about that. Let's go to Theo, see what he's got to say.

Theo Geurts: Thanks, Chuck. And I'm sort of following Marc's thoughts there. I mean, it all boils what is the purpose and if we look at expiration dates, creation dates, and update dates which are available through the thin Whois, that is something you can look up at your control panel at your registrar. So there is a solution with different technical means there. So why do we publish that in public? There is no justification for it because you can already look it up at your registrar's control panel.

Is it a violation of law? Doubtful. Could there be situations that there would be a violation of law? Maybe. But that is actually very hard to determine for us as a working group unless we are extremely fluent when it comes to the GDPR and we know exactly the ins and outs. So the question is, and I'm reversing this, why would you display it in the first place if it could be a problem? Because from my point of view, there might be a purpose and if there's a purpose can you solve it by other any technical means without displaying it in

a public directory? If yes, then don't use it. That's going to make your life a whole lot easier to tackle all these issues. Thanks.

Chuck Gomes: Theo, I'm going to - bear with me on this because I don't mean to be too difficult on this. But we could actually argue…

Theo Geurts: Oh yes.

Chuck Gomes: …that we don't need Whois at all. And yet there are lots of needs that are met by it. So, I mean, really there's nothing that says we have to have a Whois. So I could…

Theo Geurts: May I answer that one?

((Crosstalk))

Chuck Gomes: …argument and say well, we don't really need Whois, nothing written in stone that we have to have a Whois. So go ahead, Theo.

Theo Geurts: Thanks. And I didn't want to be very blunt or rile people up here or ruffle any feathers, but if you look at the Whois and you ask me that question directly, "Do we need a Whois?" Then my answer is not really because what we are talking about is a domain name, which is a commodity that we are all using and a lot of people are using.

And if we look outside of the ICANN bubble and when you look at your smart phone subscription, can you look up a cell phone number in a public directory and see when you started with your subscription, when you upgraded it or when you transferred it to another telephone operator? When is your subscription going to expire? No, it's not there. It doesn't exist.

And there's probably a pretty good reason for it. And I'm not saying that I know exactly everything when it comes to privacy laws, but there are so

many countless examples outside of the ICANN silo that don't do this and they already - these companies - they already had tons of experience with dealing with all these privacy laws. So I think what we are doing is sort of catch up in a really compressed timeframe and that is causing a lot of friction and we are sort of in this position now. But if you ask me do we really need Whois? I think I can use any other technical means to accomplish what everybody is trying to use.

It would be harder, yes, absolutely, and how are we going to deal with abuse? Another good question. I don't have the answers for that. But point blank from a technical point of view, no, we don't need a Whois. Thanks.

Chuck Gomes: Thanks, Theo. Marc, do you want to add anything?

Marc Anderson: Thanks, Chuck. I guess, you know, I'm guessing you're not following along in chat especially since it's pretty active. But, I mean, Lisa sort of hit on part of what I was trying to get to is…

Chuck Gomes: Yes, I did see that, yes.

Marc Anderson: Yes, so for example, you know, the Whois server and referral URL fields, these are fields that are legacies of the thin thick model. And if you're not operating an RDS in a thin model, then they don't really serve any purpose and it's not necessary to have those, in fact, they don't - not only is it not necessary, it's extraneous. So, you know, I think that was part of what I'm struggling with as far as, you know, the question and, you know, whether it, you know, whether focusing just on thin data right now is the right approach. But, you know, I think that's more the point I was trying to make. Thank you.

Chuck Gomes: So to follow up on that, Marc, this is Chuck again. If we as the working group, can identify legitimate purposes for each of these thin data elements, okay, you have any problem with them displayed publicly?

Marc Anderson: No, again, does publicly mean there can't be any controls on it - in front of it. I think you're saying we can have, you know, we're still open to having controls on it, right?

Chuck Gomes: What do you mean by controls? Is it gated?

Marc Anderson: Some…

Chuck Gomes: Only some people can have access? I'm going back to the Expert Working Group and the way they dealt with it. The Expert Working Group - and somebody from the Expert Working Group help me out here, the - if they identified some data, I believe, that wouldn't be gated, okay, everybody could see it with, you know, certain logistical constraints and so forth, other data would be controlled, would be only certain certified people would be able to see it. That's what I'm getting at. Anybody from the…

((Crosstalk))

Marc Anderson: And I think, you know, Chuck if…

((Crosstalk))

Paul Keating: Chuck, this is Paul Keating, I'm sorry to barge in. But this is Paul Keating. I see the difference is - there's a limitation on accessibility for commercial reasons. I don't want someone to scrape my database. Okay? As opposed to other restrictions which are I want to know if you have an appropriate purpose for asking, okay?

Chuck Gomes: Yes.

((Crosstalk))

Paul Keating: That's kind of what I see the difference of being here. And so I would - maybe you could reframe the question to speak or in that regard so we don't get too far afield.

Chuck Gomes: Did that make sense, Marc?

Marc Anderson: I was on mute. So I guess another question, you know, let me make sure I understand the, you know, I believe the recommendation of the EWG was to do away with unlimited anonymous public access. Am I correct in saying that? Okay. Then I think, you know, I, you know, I agree with the EWG report, right, and so, you know, if your question is should these data elements be public, then I'm going to say no. Like I say, I agree with the EWG report that recommends getting rid of unlimited anonymous public access to the data.

Chuck Gomes: Yes, but so we're not in disagreement there but the - what we're really trying to find out for thin data elements should there be unlimited access to those? And you're saying no - the thin data elements.

Marc Anderson: That's correct.

Chuck Gomes: Okay and okay all right well we'll accept that. And Theo is saying the same thing. Let's let a couple people talk. Andrew, go ahead.

Andrew Sullivan: Hi there. It's Andrew Sullivan again. I seem to be talking a lot today, I'm sorry. There has been - some of this discussion has suggested that the only people who need access to some of these data elements are people who are in some sense related to the domain name itself, so, you know, the created on or expired on or expiry date or whatever, you know, you can look that up another way. But actually other operators of infrastructure on the Internet can't look it up another way. That's the reason we have this service.

So the purpose of this service originally was to enable, you know, the disconnected parts of the Internet who have no prior contractual relationship

to one another, to look one another up. And that's different from the phone system. So the reason that we have this service is precisely so that people can say hey, wait a minute, this site isn't working and I need to contact the people and I'm an operator of some other infrastructure, and so I have a way to look that up.

And as far as I can tell there's nothing in the thin Whois data, and that includes the referral URLs because despite the fact that lots of people are not using thin systems anymore, it's there in support of the operation of the infrastructure. So I think the - maybe the - a friendly amendment is to say do you agree that whatever the thin data is, if it is necessary for somebody to operate infrastructure on the Internet, then, you know, that is acceptable as public access. And then maybe we can have an argument about whether, you know, the created on date is really necessary or, you know, the referral URL is really necessary if you're running thin infrastructure or whatever.

But the point is that it's - all of this stuff is necessary for somebody to run some infrastructure on the Internet. And I think that that's the reason that it should be ungated public access.

Chuck Gomes: Thanks, Andrew. Paul.

Paul Keating: Andrew, I'm sorry, but what you just defined was an example of gatedness, okay? I have to show a reason for access to the information, which is contrary to what the whole - I'm sorry, the question at issue is should anybody and their uncle for whatever reason because today's Tuesday, I want to see it, I get to see it. That's the question. Okay? I'm sorry, but that's as clear as I could try and make it and I apologize for being aggressive, okay, and the volume of my voice. Okay?

What we are discussing here is status, creation date, expiration date, name server, whether it's - when was it last updated and what is the location of the registrar Whois? That's what I wrote down when the definition was in front of

me on the screen. It's no longer in front of me, but I would like it to be if staff could put it back up on the screen, I think it would be very helpful for the conversation. Okay?

Those are the items, 1, 2, 3, 4, 5, 6, 7, the registrar, 8 items that we're talking about for thin Whois. That's all we're talking about here. Okay? Now I will tell you that as a lawyer I use just about every single one of these every other day when I buy or sell a domain name, I want to know when it's been changed, I want to know when the last update is, I want to add that to my historical Whois records, I want to know what is happening to this domain name so I can tell my client whether or not they're dealing with the actual owner or not.

I want to know where the name server is pointed out. I want to know when it's last been updated. I want to know who the registrar is because my client may have a claim and they might want to know whether they have to go to India to deal with an issue or whether they're dealing with it in California or Spain, where I'm presently located. Okay?

I want to know when the expiration date has occurred. When was it created? When was it created? It's important when it was created. Is it preexisting a trademark claim or not? I mean, these are all vitally important statistical data sets that have no personal identifiable information in them at all which is the only issue with the privacy directive in the European Union. It is personally identifiable information that those laws…

((Crosstalk))

Chuck Gomes: Okay, I'm going to have to cut it off because we're out of time.

Paul Keating: Okay.

Chuck Gomes: Thanks, Paul and sorry to interrupt.

Paul Keating: That's okay.

Chuck Gomes: I am…

((Crosstalk))

Chuck Gomes: …concerned - I think we're trying to be so precise…

Paul Keating: No.

Chuck Gomes: That - no, I'm not talking to what you're saying, I'm really talking to Marc and Theo, we're trying to be so precise, and I'm not sure it's adding value to helping us reach consensus. If I could believe that it was adding - constructive and meaningful distinctions that we're making that will make a difference in terms of where we're heading, I'd feel a lot more comfortable. I'm just not seeing the added value of being so precise. But we can't continue the discussion now. We're out of time. We will continue it in our next meeting.

And hopefully we'll come up with some ways maybe to put a wrap on this better than we have today. My questioning certainly hasn't succeeded in that regard but we'll - maybe the rest of the leadership team can help me figure out what to do or if any of you have ideas, that's fine. But I'm really not seeing this being a very constructive discussion in terms of helping us to reach some sort of a decision in terms of what data can be displayed to anybody without qualification versus that.

And whether it's needed or not, does that matter? As long as there's no harm, as long as there's no laws broken, as long as we can come up with a legitimate purpose? I don't know, it's not making sense to me why we would spend so much time on this. But we'll keep trying.

Lisa, you had your hand up. Please jump in.

((Crosstalk))

Chuck Gomes: I don't know what happened to Adobe here, it seems to disappear for me, but go ahead, Lisa.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. My takeaway from what I'm hearing from this discussion is that we're still struggling with the sort of highly interdependent and unfortunately that means iterative nature of the questions that are in front of us. The reason that the process framework laid purpose out first was so that we could hopefully reach some agreement on what the legitimate purposes were then go to data elements and look at the data required for that group of purposes and then go to the question of access and determine whether access would be public or something other than public for each of those data elements. So that was sort of a waterfall model in the process framework.

I think what we're struggling with here is that by jumping ahead to access, I hear Marc struggling with well, is there a purpose for some of this data in the first place? We're just going to have to break off a smaller piece, make some working assumptions and then try to answer that question. If we continue to try to answer all three or four of these questions at the same time, we're going to continue to spin. And I guess any feedback on how we can break this apart in a way that we can take one small piece and try to answer that one small piece and use it as a building block would be really welcome.

Chuck Gomes: Thanks, Lisa. Well, we're over time.

Paul Keating: I know we're over time.

Chuck Gomes: Our next meeting will be at the same time next Tuesday. We will continue. I welcome discussion and encourage discussion on the list in the meantime. Anybody that can help me understand the value of the concern - does it really

matter the things that we - in the long run in terms of our bigger objectives? Does being this fine, I mean, if you can - I'd love you to help me understand how this is helping us by getting to this fine detail in terms of whether it's needed or whether it can be obtained somewhere else or, I mean, I'm all for dealing with real issues.

I haven't heard any issues that were very convincing to me in terms of not displaying any of this data that makes a difference. So please, if you have suggestions there let me know. It doesn't mean what you said was wrong; I'm just not sure it's helping us. And that's where I'm struggling. So anybody that can help me understand that I welcome that.

Lisa and staff, other vice chairs, anything else we need to cover today? My Adobe screen's gone blank so I'm not seeing anything on that.

Lisa Phifer: Chuck, this is Lisa Phifer. I just put a link in chat to the current version of the working draft which we added a new Section 5 on access. And I really think it might be helpful for those on this call to go have a look at that new Section 5 and in particular the EWG text that tried to tackle some of these same questions. Not necessarily that the answers are going to be the answers this working group comes up with, but it really might help to gel the concepts that were raised today by taking a look at that and how at least that group chose to tease apart the problem.

Chuck Gomes: And, Lisa, that might be a good place to start next week.

Lisa Phifer: Yes, it might be.

Chuck Gomes: Okay. Good, thank you. Anything else? Well thanks, everybody. And we will pick up there next week on the list in the meantime. Meeting adjourned. And the recording can stop.

END