ICANN
Transcription
Next-Gen RDS PDP Working group call
Wednesday, 19 April 2017 at 05:00 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-19apr17-en.mp3**

AC recording: https://participate.icann.org/p6e1urc6y3e/

Attendance on wiki page: https://community.icann.org/x/C8PRAw

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

Coordinator: Recordings have been started, Nathalie. You may now begin.

Nathalie Peregrine: Thank you ever so much, (Jamie). Good morning, good afternoon and good evening, everybody. And welcome to the Next Gen RDS PDP Working Group call on Wednesday, 19, 2017. In the interest of time there will be no roll call taken today. We'll be taking attendance from the Adobe Connect room only therefore if you are now connected via the telephone only and not able to join the Adobe Connect room, could you please make yourselves be heard right now? Hearing no one. I'd like to remind you all to please remember to state your names before speaking so that they appear correctly on the transcription. Thank you once again, and over to you, Chuck.

Chuck Gomes: Thank you very much, Nathalie. And welcome to everyone to our working group call today. Does anyone have an update to their statement of interest? Susan, go ahead.

Susan Kawaguchi: Thanks, Chuck. It's Susan Kawaguchi for the record. I have left Facebook. I'm no longer a Facebook employee and I'm working as a consultant. And I've updated by SOI to reflect that.

Chuck Gomes: Thank you very much, Susan. Much appreciated. This is Chuck. Anyone else? Okay, then let's go ahead and get started with Agenda Item Number 2, and we'll come right back to Susan for an update on the ccTLD questions that are being considered regarding the data protection issues.

Susan Kawaguchi: We've gathered together about 10, 12 questions. I didn't get this out to the sub team in a timely manner, I didn't get it out until this afternoon. So Alex has weighed in again and I'm just going to give it one more day for the rest of the sub team to provide their thoughts, and we're going to revise a few of the questions and then - and also develop a strategy for reaching out to the ccTLDs, so hopefully have something tomorrow to the whole working group.

Chuck Gomes: Thank you, Susan. Let's go to David Cake. And, David, can you give us an update on the small group of you, Mike Palage and Andrew Sullivan, on the definition of authoritative?

David Cake: Can you hear me?

Chuck Gomes: Yes.

David Cake: Yes, I'm going to have to apologize, the small group did not get (unintelligible) period probably because I was essentially not on the Internet for most of that period. I think - first I'd like to note, which I should have noted last week but Nathalie (unintelligible) on that group, volunteered, and so far I think we had - we seem to be heading towards consensus that we are probably not going to produce a definition of authoritative.

The use of that word in other context, both legal and technical within the RFCs, where - and look at the RFC, which of course is that Andrew

(unintelligible) they basically - reveals that the use of that word within technical definitions is highly specific to the DNS so not really useful for directly using within the RDS and just likely there may be some confusion because there are a number of subtleties.

So rather than produce a definition of authoritative we're probably going to try and produce a form of words which captures the same concept but we have not yet finished doing that.

Chuck Gomes: Thank you, David. Now is it - this is Chuck. Is it possible you will have that by our next meeting?

David Cake: I should imagine we will have something by the next meeting.

Chuck Gomes: And it'd be great if we can get it to the working group at least 24 hours in advance of next week's working group meeting. So if that's possible that would be much appreciated.

David Cake: I should think so. And I mean, the Easter period is over, we'll be back on track to working as usual.

Chuck Gomes: And you guys will - this is Chuck again - I assume you will provide your explanation of the route you're going somewhat like you said today, so that everybody next week and on the list will be able to see your rationale, and then we'll discuss that - your approach in the working group call next week?

David Cake: Yes.

Chuck Gomes: Thank you. Okay, let's go to Agenda Item 3 and start discussing the answers from the data protection experts. In the poll that we did this - or last week, we took the answers for the first two questions and just asked each of you to do a couple things in that regard, share any possible key concepts that you've

picked up out of that and also identify any clarifying questions we may need to pursue further with regard to the answers that were given.

So let's - we've got the results up in the screen. And it looks like everybody has the ability to control that on your own now.

((Crosstalk))

Olevie Kouami: Good morning.

Chuck Gomes: I'm sorry, I didn't understand that.

Olevie Kouami: Yes, Daniel online. (Unintelligible).

Chuck Gomes: Oh Olevie, okay.

Olevie Kouami: Yes. (Unintelligible).

Chuck Gomes: Okay, thank you. And please mute when you're not talking. It sounds like when you and I are both unmuted that we get an echo. So and if you want to speak up, Olevie, please do so and I'll get you in the queue as soon as I can.

So all right so you can see who participated in the poll. We won't go through that. You can see we - 24 people responded. We're going to come back to Question Number 2 later, we're going to start with - actually we're going to start with Question Number 4, the last one which is the second question in the 19 questions that we asked the data protection experts.

So if you can scroll down to that question you'll see it there starting on Page 7, and we'll - we're not going to go through the comments because there are a lot of them, okay, but instead what we're going to do on this one is, if you'll scroll down to the bottom you'll see I think - and hopefully it's the same for

everybody, the blue font there, we have a summary that staff prepared for us of common themes or key concepts that responders suggested.

And we're going to talk about those right now, I'd just like to get the reaction of everyone on the call that's willing to express it, what you think about these key concepts that were identified by working group members. You can see under A there, allowing people to get in touch with a domain name holder is a legitimate purpose. That's a key concept identified by three people. You can see it'll be commenters 1, 2 and 7 there.

Curious what you think. How many of you would agree with that being a key concept out of these answers? And Tim O'Brien, you're welcome to speak if you want. I was going to ask people to just put a green checkmark if you agree with that being a key concept.

And then while we're doing that, how many of you would disagree with that as a key concept? So leave your green checkmarks up, please, ok? And I'm going to call on you in just a second, Tim. But if you disagree with that as a key concept you can put a red X in the Adobe chat room and Olevie, if you have a - want to express your opinion you'll just have to speak it out.

In the meantime, Tim, go ahead. Tim O'Brien?

Tim O'Brien: I was trying to hit the - yes, this is Tim O'Brien…

Chuck Gomes: Okay.

Tim O'Brien: …I was trying to hit the affirmative to that. But certainly this is something I do, on a daily regular basis, due to my work duties and also personal research. Trying to go through, yes, sometimes (unintelligible) hosting provider do work and sometimes are effective. But a lot of times, going directly to the Website owners in regard to a security vulnerability or a problem or the Website being

compromised, has a much better, much more responsive feedback to that sort of effort.

Chuck Gomes: Thank you, Tim. This is Chuck again. Scrolling down it looks like - okay so Stephanie, you would disagree with that. Would you like to comment on that?

Stephanie Perrin: Hi, can you hear me? It's Stephanie Perrin.

Chuck Gomes: Yes.

Stephanie Perrin: I didn't - I didn't actually (unintelligible) because…

Chuck Gomes: We seem to have lost you, Stephanie.

Stephanie Perrin: Is this better?

Chuck Gomes: Yes.

Stephanie Perrin: Not sure what happened there. I didn't actually fill out the poll because I found that the question like disentangling what you learn from this rather full answer into separate concepts in my view, nullifies it. So, yes, at some kind of an intrinsic level, you want to contact the domain name holder, but it's qualified by all these other concepts. So if you say yes, contacting the domain name holder is okay, you're disentangling it from all the caveats with it. That's why I'm objecting.

Nathalie Peregrine: Nathalie, you may be on mute.

Nathalie Coupet: Chuck, are you there?

Chuck Gomes: My apologies, I was on mute. Jim Galvin, would you explain why you disagree please?

Jim Galvin: Thank you, Chuck. Jim Galvin for the record. In this, you know, case of is contacting the domain name holder a legitimate purpose, I guess I struggle with that question for the same reason that Stephanie does. I find that, you know, yes, one might need to be able to contact them, but I don't think that it needs to be a direct contact. And so, you know, I think that having to do that through a layer, I see that's a comment which comes up later - I mean, the idea that I should have to be able to get right to the domain holder, I struggle with why that should be a legitimate purpose.

You know, if I have to go through the registrar, for example, that would seem okay to me, you know, without any questions. But, you know, Stephanie calls them caveats, I think that there are, you know, legitimate concerns in all of that. And I guess I'm just not sure how to apply all of those legitimate concerns and agree with this statement at the same time. So that's my comment, thank you.

Chuck Gomes: Thanks, Jim. Chuck again. Note that the people who put this as a statement, and this isn't the way all of them exactly worded it, but it doesn't say how to get in touch with them so it could be through a third party, it could be through gated access, some other thing. But thanks, Jim, that's helpful. Is there any - and then, Rod, go ahead. Please speak.

Rod Rasmussen: Rod Rasmussen here. So I think, you know, we've got a generic concept of being able to contact the - a domain holder. And when you - and that's kind of a meta concept. When you break it down it's really contact the domain holder or the representative for a particular type of purpose, right? So in the case of being able to so for example transfer a domain name from one party to another, oftentimes you will want to talk to the holder of that domain, but in some cases you may talk to their legal representative.

For cases of needing to get some sort of technical issue addressed, say that domain is a infrastructure domain that is not providing the services it's supposed to other domains on the Internet, you may want to talk to a

technical representative but you may want to talk to the holder. So this gets into - and I think what Stephanie is getting at and what Jim's getting at is that, yes, in general, as an overall concept, the domain holder is the placeholder for the concept of getting a hold of somebody that can make decisions around that domain name.

But then it breaks down into each individual purpose I think to deal with the various data protection privacy etcetera, etcetera, etcetera that we've been talking about here for the last couple of months. So I think that what we've got as a general concept we - in general we agree with but the devil's in the details when it comes to how that is actually done, right? So I'm not sure how you get past that. But I think - I don't think there's a disagreement around the overall concept, it's around how do you define that and how do you put that on paper? Thanks.

Chuck Gomes: Thanks, Rod. It's Chuck again. So is there anybody that disagrees with the general concept of needing to get in touch with some person associated with the domain name understanding that there will be some caveats and there's some more work to be done in that regard? If you would either speak - raise your hand to speak or put a red checkmark in there?

So at least for those of us on the call, it looks like there is agreement on kind of the way that Rod just expressed it but also Stephanie and Jim. Okay, let's go to B. And if all of you would clear your checkmarks and red Xs if there are any still in there, I would appreciate that.

So B says proportionality needs - I think that's supposed to be - to be assessed in relation to each data user. Notice there was 1, 2, 3, 4, 5 different people basically said this, that may not have been their exact words, but that's kind of what they picked out of it, proportionality needs to be assessed in relation to each data user. How many of you would agree with that as a key concept?

And can we assume that for all of these separating them out leaves some to be desired, okay, we understand that. So these things shouldn't be thought of just in isolation even though that's what we're doing, okay, kind of isolating them so that we can talk about them.

So let's assume that this statement would be taken in the context of the broader answer that's given and that we will have to fill in the details to all of these things as we move forward. So does anybody - how many of you agree with the as a key concept. Put a green checkmark in or a red X.

And, Stephanie, I see the red X for you. Is this the same reason that you put a red X for the one in A? And that's a question - yes, go ahead, Stephanie.

Stephanie Perrin: Basically yes, Chuck, if you can hear me. Proportionality has to be applied to every aspect of how you interpret this. So…

Chuck Gomes: And that's what I just tried to say…

((Crosstalk))

Stephanie Perrin: …it applies to each user - well, I think my objection to trying to pull these apart if we pull out that it applies to the users it also applies to an operation with a data element. So, you know, if you say one and you don't say the other then it implies that it applies only to that one.

Chuck Gomes: Okay thank you. I only see one green checkmark. Can I assume from that that there's only - that only Sam supports this as a key concept with the caveats that Stephanie mentioned again? Okay, so we don't have a lot of strong support for B. All right, that's fine. Let's clear the marks again, green or red, and go to C.

ICANN needs to distinguish between individual person and legal person registration data. Okay. I assume that means registration data associated

with either a legal person or an individual person. And is that - quite a lot of - let's see, what is there, about eight people - about 1/3 of those that responded mentioned something along this lines. How many of you would agree with that one even though it's in isolation and we know we need to look at the bigger picture? Okay.

We have several - and Stephanie, we know why Stephanie disagrees with that one. And, Jim, is your disagreement the same as well?

Jim Galvin: No, Jim Galvin for the transcript. I think what concerns me about this statement is it feels like an issue which is subject to a local concern as opposed to a global concern. And when I think about the RDS, you know, I'm thinking about what we need to do in a global context. So, you know, and I don't think that this particular statement and this distinguish that applies in that larger context. So that may just be me and maybe we just need a little more discussion but that's what's on my mind. Thank you.

Chuck Gomes: Thanks, Jim. This is Chuck again. Much appreciated. And let me pursue that just a little bit, Jim, and others feel free to jump in. It seems to me when we're talking about laws and we still have to define, you know, the interpretation of the laws including what the data protection experts have presented, but there aren't too many laws that are probably going to be universal, in other words, globally applicable.

So isn't it fair to assume that going forward we're probably going to have to - we're probably not going to have too many things that apply across the board globally when it comes to laws, that apply to the RDS. And so, of course that's one of the advantages of RDAP, and the ability to localize where needed. And I suspect that that will be - now we - in Copenhagen, we're listening to data protection experts from Europe. And they don't have the same requirements as other geographies around the world.

So if we try to do everything on a global scale, it's going to be very minimal what the RDS will have if we take the lowest common denominator. On the other hand, if we take the largest common denominator, anything goes, right? So I'm curious - it seems to me we will have to localize at some point because registrants and registrars and registries are going to have abide by applicable laws even if they're not global.

So, Jim, do you want to respond to that?

Jim Galvin: So thank you, Chuck. Jim Gavin again. I think the only thing I can think of to say is being able to access the data is certainly one thing, I guess I'm just trying to understand you know, why it's important to be able to distinguish if the domain holder on a, you know, global level is an individual or something else. I mean, this explicitly says, you know, individual person and legal person. I guess I don't want to read too much into the words that are chosen here, you know, maybe just the idea that I need to know if it is actually a person of some sort versus a corporation I think that's the usual distinction we make. I'm having trouble, you know, understanding why that's an important thing on a global scale. I now have the domain holder, and I've got some contact information through whatever other means I got, you know, why is it important to have this detail?

And I'm also thinking forward and I'll add one other quick thing, which is what this means is that becomes something that has be collected because again here we're conflating two points, one of which is collection and one of which is publication, and I think we're suggesting here that on publication we want to know what that is. And I point out it's just interesting to point out that this is not something we collect today, so again, this becomes a change that has to be dealt with down the road, not that that's a bad thing but I just think it's important to keep that in mind too. Thank you.

Chuck Gomes: And thanks, Jim. Chuck again. And I think you're right, if this distinction does need to be made for some jurisdictions, that information will have to be

identified with the registration so that potentially could become a requirement down the road. We haven't gotten there yet, but I think you're absolutely right. But back to your question, why do you make that distinction? I think the data protection experts told us why you need to make that for European law because the global data protection requirements that are going into effect a year from now apparently are for individual people, not legal persons.

So based on that jurisdiction's laws that are coming into effect, and may somewhat already be in effect, that's why you would have to make that distinction at least for that jurisdiction and their laws. Greg Shatan, go ahead.

Greg Shatan: Thank you, Chuck. Greg Shatan for the record. The - a couple of points. First, you know, clearly we're listening to EU data protection regulators as a rough turn. I hate calling them experts because it makes it sounds like they're the only experts. Obviously one hopes they're, you know, good at their job and expert in it, but there are a variety of different types of experts around laws just like the only experts around antitrust laws aren't the Department of Justice and the Federal Trade Commission. And if one listened to only them you would never try to, you know, a merger or do a bunch of other things that are actually allowed. But that's a side point.

I think what's going on here of course is that we are trying to pull out concepts from the answers that we were given, so this is not just, you know, a question of, you know, where do these - where they came from? They came from the regulators' answers. And because, you know, at least that regulation scheme it's important to distinguish, not because the person who's trying to contact an individual or domain holder needs to know whether they're an individual or an entity but because whatever policy we make at least as far as it applies to things like that, are going to be policies that we'll need to distinguish.

And, you know, given that we're talking about the concept of privacy, I think it's probably not merely local that there would be distinctions made between

actual persons, human beings and their rights to privacy and the rights to privacy, whatever they may be, of legal entities, who I don't think generally enjoy a right of privacy under any regime or many regimes obviously, no place to generalize here off the top of one's head at 1:30 in the morning.

But in any case, I think we will probably need to make - look at that distinction more generally with regard to, you know, what types of access and publication and the like there will be available to us. So it seems to me to be an appropriate distinction to capture, appropriate concept, that will probably come back and be very applicable, you know, in a number of contexts throughout our work. Thanks.

Chuck Gomes: Thank you, Greg. This is Chuck. Stephanie, I assume you tried to have your hand up before when it was just a red X, go ahead, please.

Stephanie Perrin: Thanks very much, Chuck. Yes, indeed, I did. Once again I think that we are pulling this particular concept out of context because this was in answer to a question about 6.1B, I think it was, and it said for instance, ICANN needs to make this assessment. The problem is - arises largely depending on whether you're thinking in terms of whether a domain registration is being used for commercial purposes or whether the individual registering it is acting on their own will, acting as an agent for a company, acting as a small business, acting for a commercial purpose. Those are all different.

And we went into this ad nauseum on the PPSAI Working Group. And I think we managed to get the point across that figuring out how a person registered a domain name at the point they registered it, if they are not acting as a corporation, I mean, obviously if someone's working for Facebook they're identified as someone working for Facebook and they register umpteen domains and they say - list the address as Facebook, that is kind of clear that that's a corporate entity and someone working for it. And if they're not operating in Germany then they don't need to have an express consent to have their name listed as the contact person on the Internet, for the Whois.

But that doesn't pertain to most of the other registrations where it's an individual acting as an individual, picking up a cool name, they don't know what they're going to use it for, they don't know whether they're going to use it for their company, their small business, whatever. So I think this whole thing, you know, is just too nuanced to strip it out as a key concept.

Yes, data protection only applies to individuals, but there's a whole lot of caveats on that. It also applies to employees in certain jurisdictions and there has to express consent. So if you're talking about disclosure that's different than collection. I think I'm probably making the same point Jim made, but that doesn't stop me from trying to make it again. Thanks.

Chuck Gomes: So, Stephanie, this is Chuck. I'm going to pursue that just a little bit further so you can take yourself off of mute again. But so I hear you saying that, yes, there - we need to distinguish between individual persons and legal persons. Now I don't think anybody will disagree with you that there are a lot nuances to that and we're going to define those.

But I do hear you agreeing with C that - there's going to have to be, at least for the European regulation, there's going to have to be some distinguishing between these two categories because the GDRP - I always get the letters wrong - it applies to individual persons. Am I correct on that?

Stephanie Perrin: Yes, you're correct on that.

Chuck Gomes: Okay thank you. I just wanted to confirm that.

Stephanie Perrin: Yes, you're correct on that. Yes. But that's not the only reason that entities might be entitled to confidentiality.

Chuck Gomes: Oh I understand that. I didn't say that it was. And also, as you'll recall in the session in Copenhagen, one of the experts pointed out that even if someone

is an individual person, there can be reasons for disclosing their information under certain circumstances as well. So just because somebody is a natural person doesn't necessarily preclude any disclosure of information under certain circumstances. So let's go to Alex.

Alex Deacon: Thank you, Chuck. This is Alex. So I guess just quickly here, the comment I wanted to make was in response to Jim's comment from a while back. And I think - I appreciate everything he said but I think it's important to remember the context of the original question we asked the commissioners and the specific responses we received back from the EU data protection folks as a subset of the panel.

And really the focus of the current conversation or at least C in the blue box, in the summary that staff put together, is specific to the question we were asked to answer, or respond to in the poll, which was what are the possible key concepts suggested to responses in Q4?

So I think this is all interesting conversations but I think really, you know, if you take that question kind of at face value then my reading of the responses from the EU data commissioners to our questions that this is a pretty key concept with regard to privacy in at least the EU experts - the EU jurisdiction. Thanks.

Chuck Gomes: Thanks, Alex. This is Chuck again. Marc Anderson, you're next.

Marc Anderson: Thanks, Chuck. This is Marc Anderson for the transcript. This is a really interesting one especially for 1:30 in the morning for my time at least. You know, and I think it's something, you know, that, you know, it's worth spending time on because, you know, I remember the Privacy and Proxy Working Group had to, you know, consider whether or not privacy proxy, you know, should be accessible to, you know, natural persons only or, you know, legal entities as well.

And I think that was something they struggled with a little bit and was a little bit of a hot topic for them. So, you know, responding to, you know, ICANN needs to distinguish between individual persons and legal persons, you know, I think we as a working group need to make a decision, you know, are we going to treat individual persons and legal persons differently?

You know, and, you know, I think there is a possibility of doing that. I think some TLDs, if we look at ccTLDs, and even some gTLD is, they do in fact treat, you know, legal persons and natural persons differently. But for the vast majority of TLDs, you know, I'd say they do not, they don't distinguish between the two.

So, you know, I think, you know, this is something, you know, it's worth spending time on, you know, it's worth us, you know, been deliberate in making the decision, you know, for the purposes of, you know, the Next Gen RDS PDP, you know, should, you know, should domain registrations to, you know, natural persons versus legal persons receive different treatment in the RDS?

You know, so, you know, I'm not, you know, I'm not advocating for one position or another, but I think as far as concept goes, I think this is something we need to make a decision on. Thank you.

Chuck Gomes: Thanks, Marc. And I'm going to follow up with you as well. This is Chuck. So if there are legal jurisdictions that require that distinction to be made, do you think we still have the freedom to decide whether to do that or not or do we have to comply with the law?

Marc Anderson: Well, Chuck, you know, you pointed out that, you know, certain, you know, certain privacy laws treat legal persons and natural persons differently. But that doesn't necessarily mean we have to make a distinction, right? You know, so I'm not, you know, I guess my feeling is the one doesn't preclude the other. Maybe, but I don't think…

((Crosstalk))

Chuck Gomes: So in other words you think…

Marc Anderson: …they're mutually exclusive.

Chuck Gomes: Marc, so you think that if - even if there are jurisdictions that require that distinction to be made, that we could still refuse to make that distinction?

Marc Anderson: I'm not sure they - well, you know, I'm not an expert on this but, you know, I don't think…

((Crosstalk))

Marc Anderson: I don't think they - that's what they're saying. I don't think they are saying that we are required to make that distinction. I think, you know, what we've heard is that from the day the commissioners is that in many cases the data privacy laws apply to individual persons or natural persons, not legal entities. I did not hear them say we are required to make that distinction.

Chuck Gomes: Okay, I'll leave that at that point. Susan, you're next.

Susan Kawaguchi: So I'm going to disagree with Marc. I think that if an entity self identifies as an entity, and it's clear in the record, for example, Facebook Inc, that it is an entity and not an individual, then we can't convey natural persons data privacy rights to that entity especially in Europe because Europe makes a big distinction between natural persons and legal versus I guess or legal entities.

So if they have self-identified then we would have a duty to display that information in a way that complies with the law in that government. So I think we do have to pay attention to this and whether or not it's marked in the record as a natural person or a legal person, you know, for all to see that's

one thing. But if the record detects a sort of a declaration, a self-identification of a legal entity, then that data should be treated differently to comply with the law.

Chuck Gomes: Thank you, Susan. Chuck again. Jim, your turn.

Jim Galvin: Thank you, Chuck. Jim Galvin for the transcript. I want to clarify my position from earlier and just observe, I've been swayed a little bit by this discussion here and I do understand something a little bit better. I acknowledge that I think that we have to collect the information as to whether or not a domain name holder is a natural person or not. We might need some more discussion on the phrase that we are going to use there and what it means so it has global applicability.

I'm still not certain about the publication of that particular information so I want to draw that very careful distinction in the clarity of my position. I want to thank Rod for his comment there in the chat room with respect to this, that's what finally swayed me in that. And I do think that distinction between collection and publication is important in all of this. That's sort of my favorite little hot button to bring up in these discussions. So thank you, I hope that's helpful.

Chuck Gomes: Yes, it is, Jim. Thanks. And again, we are going to have to get into, you know, collection and display and gated access and all of these things as we move along. But I hear a lot of people recognizing that there is a distinction here that may be important, it needs to be defined more clearly. But let's go to Greg Shatan again.

Greg Shatan: Thanks, Chuck. Greg Shatan again for the record. So I think again this issue of natural person versus legal person is an issue that goes to how data is handled so to speak, and not so much a question of whether the particular data points needs to be published or not, although I would wonder why, you

know, where the issues would be in having it published especially, you know, in a regime where there is limited privacy rights if any or legal persons.

And in any case probably easy enough to figure out if their name ends in Inc, Corp, or SA or SPA, that they're some form of a legal person. The primary, you know, reason to collect this information is because it influences what legal obligations there might be with regard to privacy. Or the opposite, there may be legal obligations with regard to transparency, which seems to be a very popular concept everywhere but this working group.

And, you know, certainly there are various requirements, you know, for transparency knowing who you're dealing with, that, you know, very much fit in with, you know, Whois or RDS concerns as well. So but I think on this particular point, you know, the issue is that this is a - this is a metric or information point that influences how other data is handled. Thanks.

Chuck Gomes: Thank you, Greg. Let's go to Alan Greenberg next and then we're going to go to D, so go ahead, Alan.

Alan Greenberg: Thank you. Commenting on something Susan said, and actually Greg just alluded to it, the way I heard it, and maybe I misheard, is that if you are a legal person we have an obligation to make information available. I thought that we were really talking about if you are a natural person, we may have, depending on the jurisdiction, have an obligation to not disclose information. But is it the case that there are jurisdictions where we may have an obligation to disclose if someone is a legal person?

Chuck Gomes: It's a good question, Alan. It's something we'll have to look at down the line I think. But very good question. Let's go to Question D. Now Question D is kind of unique because it's really one of our questions, it may be less of a key concept than a question that we are going to have to deal with because one of our first five questions is gated access, which is what this one is all about.

Now I'm not disagreeing with those that put it as a key concept in the sense that there are several instances in the answers to our questions where they refer to layered access. I don't think they ever use the term "gated" but they're essentially saying that. So we can talk about this one, D, but we're going to - we absolutely will have to talk about it when we get to gated access.

It is true I think, that the experts that answered the questions that we asked him slide or even stated in several cases that a solution to the problem might be layered access, as they I think referred to it or as we call it now gated access.

So I will pause to see if anybody wants to comment on that. I don't want to spend too much time on this because we're going to have to actually get to that. And again I want to re-emphasize what those of you that pulled this out dated is correct, I saw it too in several cases. So if anybody would like to talk just raise your hand. And, Alan, is that a new hand? Thank you. Okay, I'll pause just a few seconds and then we will go to E.

Tim, you're disagreeing with what?

Tim O'Brien: So this is Tim O'Brien for the record. This one aspect here bothers me in having this layered or gated access, I understand this is the focus here, but this is what in limiting the access to this information is going to limit or prohibit individuals from being able to get this information for legitimate purposes. And I take issue with that.

Chuck Gomes: And can you give me an example of that please?

Tim O'Brien: So, a good example for that is finding a particular Website that is compromised or being spammed or doing malicious purposes of no intentional of the Website owner or the web host or what not. And for those individuals like myself that not just do this for a day job but also do this at

home on our own personal time in trying to help clean up the Internet, and for lack of a better word or phrase, you know, trying to prevent the neighbor from - neighbor's dog from pooping on our yard, right?

How would those individuals like myself and others that I know in the information security industry be able to get access to this information to communicate with these web hosts, with the Website owner, with the domain holder etcetera, to try to help them out with these sort of situations?

Chuck Gomes: So Tim…

((Crosstalk))

Chuck Gomes: …it's Chuck. What you're saying then is if you have what you believe is a legitimate purpose, and maybe most of us would agree with you, that that's a good purpose, then you should be allowed to do that even if there are some laws that may be violated in doing that? Now I'm sorry for being so blunt. And I'm not advocating any position okay, I hope you're all getting to know me in that regard.

I'm just trying to play devil's advocate and test reasoning. But am I correct that because you're doing something that you think is good, even if there is a law in some jurisdictions that may not allow that, may not allow you to have access because it may be personal data, if you look at some of the answers, not just to the first two questions, the experts that responded to our questions talked about that and mentioned law enforcement even, let alone somebody that's not part of law enforcement. And they said that's not a legitimate reason.

I read a letter today to ICANN from the Article 29 Working Party that told ICANN some of the things they require in the new RAA for Registrars is against the law. Now, I think what I mean, my own opinion is that what

ICANN requires is good, they're trying to promote accuracy and some other things. And yet there are some things there.

So, Tim, I'll give you - I was - I'm picking on you obviously so I need to give you a chance to respond.

Tim O'Brien: Oh, no problem. Bring it on, right? So let me put this a different way. If a particular Website is attacking my company, or my particular personal Website or whatnot, you're telling me that it would be illegal for me to get the information, to respond back and trying to get them from stopping their attacks, which is also illegal?

Chuck Gomes: No, I'm not telling you that. What I'm telling you is, is that it might be illegal for ICANN to give you that information, if that information violates some laws and some restrictions. There may be other ways of getting it. So I'm not necessarily saying that, but ICANN obviously has to comply with local laws where they are operating. And so do registries and registrars. So that's all I'm saying.

And we don't need to resolve this right now. I fully respect and appreciate your need, and we need to try and see how can we best deal with that. But I'm just trying to help us all see this in a bigger context. It's not as simple as I would like it to be I know, or you would. And I probably sympathize for everything you're doing. Okay, Rod, go ahead.

Rod Rasmussen: Yes, Rod Rasmussen again. So, you know, this is a great example, and we've had many other examples over the last I don't know, umpteen calls of the difficulty in dealing with one aspect of this entire system, concept, etcetera without the context of the rest of it. And it's, you know, we've had objections and points raised from various folks tonight, but it happens all the time, and for the same reasons.

Like, hey, if you're precluding this then I can't do this, right? And it's kind of a generic hold there. And that's, you know, something we dealt with extensively in the EWG, and so I have to kind of think about this in a holistic kind of proportions. And that, yes, we've got this issue here and we want to enable, in this particular example, we want to enable people to resolve these kinds of issues, right?

So that may require not - but in order to fit into the paradigms of various local legal regimes, we may not be able to collect data from the person that actually owns the Website to enable solving this particular very legitimate purpose. What we may have to do is - may be a requirement that you designate somebody or some contact to handle those issues, and that that contact information be published so that if there is an attack or if there is a spam issue or if there is a - you know, some sort of Internet security or Internet infrastructure problem or what have you, that there is a way of doing that.

And if you don't want to designate such a person then it may fall back on to the actual owner itself to designate themselves as that if they so choose. And if we take a look at the EWG report, we kind of came to that conclusion over a many, many month process of figuring this stuff out is that, okay, we want to allow this, but we may not be able to do it kind of the way we do it today, which is very simplistically with the Whois of today.

And that's why we've got to be thinking in terms of a next-generation RDS, and this gets way ahead of where we are today. But I think a good thing to take - keep in mind as we are discussing these things is as these issues come up that seem like, well, there's no way to solve this with the current thing we're talking about is, like, okay we'll put that as a marker down so that we can come back to that and say, okay, how can we solve this problem now that we've unearthed these issues with the current way things are being done or the way that we think they should be done so that we can come up with a better solution or an alternative solution going forward?

And I think if we're following that kind of a process as we go, as marking these things as something that needs to be addressed, Chuck, I think you and the crew who are doing that, the work party leadership are doing that, but I'd like to just re-emphasize that to the rest of the group is that these are the areas that we need to put markers down and say, okay, we need to figure out how to deal with this going forward, but we don't want that to bog us down currently. Thanks.

Chuck Gomes: Thanks, Rod. I appreciate those comments. And for those that haven't looked at the EWG report in a while, I encourage you to look at it again because they really did grapple with most everything, if not everything we're grappling with. And they really did try to be constructive in addressing lots of purposes. We've recently been looking at the list of purposes that they identified that they thought were legitimate purposes.

And it includes the things that many of you want to be able to do. And they tried to come up with some ideas. They didn't develop policy but they tried to come up with some ways that maybe these things - these problems can be solved and the needs met like Rod indicated, it won't be as easy as it is today, more than likely because of restrictions around the globe that vary, but still there are these restrictions so very good.

Okay, Jim, your turn.

Jim Galvin: Thank you, Chuck. Jim Galvin for the record. I think in response to Tim, and I was listening to Rod here, there are two things that I would like to say about this statement saying that there should be layered or gated access. First a terminology issue, I'd prefer that we call this differentiated access rather than layered or gated, I think that's a more proper term here for what we're talking about.

But the two things I want to say are one, this statement is a solution in search of a problem. And, you know, we should not have this statement in our, you know, vernacular just yet. It's a solution for a potential publication issue that we are in the process of identifying by establishing what the purpose of are for collecting data, and that will inform our need for certain publication solutions. And this is one example of a way in which to solve that problem. So I just, you know, think that discussions of differentiated access are just way too early at this point. Again, I'll go back to solution in search of a problem at the moment.

The second thing that I would like to say, and this probably more directly responds to Tim's concern, you know, if there was a differentiated access solution that was chosen to support a publication problem that we may come to identify, I would expect that for the purpose that Tim has, you know, there would be a way for him to ensure that he had the appropriate credentials to do what it was that he needed. That's the role that differentiated access system would play.

So he should be able to continue doing what he's doing because it would be identified as a legitimate thing to do and he shouldn't have any concerns down the road. Thank you.

Chuck Gomes: Thanks, Jim. Maxim, your turn.

Maxim Alzoba: Maxim Alzoba. Do you hear me?

Chuck Gomes: Yes, we can hear you.

Maxim Alzoba: Okay, I just wanted to, yes, make a note. I don't think we need to reserve only one item to be like perfected or not. It's (unintelligible) we want to mark the whole domain to be potentially subject of privacy laws. I think we need to (unintelligible) where we create something which is not adjustable in the future like the current Whois. So I suggest that later or like we know that later

we come back to this question that more than one simple field, personal data or not, should be applicable.

For example, to be able to distinguish which particular fields of the record are in need of protection. So because in some situations yes, where some not so wise (unintelligible) enters his home address and his phone number and, yes, other things into the domain data. So we are able to identify which fields need to be mapped or access (unintelligible) and not just a single flag yes, no for the whole domain. Thanks.

Chuck Gomes: Thank you, Maxim. Okay going to E, there is a need to identify and document query purposes, collection, derivation only for legit purposes. This one I need a little help on myself, but I don't know if any of you do, but are there people that would like to talk about this one? Seems to be getting ahead in terms of, you know, of people doing queries and obviously that gets into display or access and so forth and whether data is collected or derived from registries and registrars.

And of course one of our tasks that we are in the middle of doing is identifying legitimate purposes for collecting the data and ultimately for more than that. Anybody want to comment on this one? Go ahead, Stephanie.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. Let's bear in mind that our purpose for collecting data is always so that we can manage the Domain Name System or whatever that purpose statement that we - the general one that we had was. But for disclosure is always something that is interrogated more fully because in principle the data protection - the data controller and processes, and that's in this case the registrars and registries, are obliged to protect the data from disclosure. Let's leave aside the fact that we've been publishing it for umpteen years.

And so therefore you always ask the purpose of the disclosure. We are talking about it as if it was a query, but it's basically a disclosure of data either

in bulk or on a fine-grained basis. So, yes, that is the question. You know, you don't disclose it. You gather it for certain purposes and you don't disclose it to others for other purposes absent a good reason.

And I really think, as much as they would be jumping ahead of ourselves, we need to unpack what we mean by tiered access - or, what's the other word, I'm sorry, it's 1:30 in the morning and I can't remember it.

Chuck Gomes: Differentiated.

Stephanie Perrin: …let's call it tiered access.

Chuck Gomes: Differentiated.

Stephanie Perrin: Differentiated or layered access. I mean, really how hard does it have to be? I know we went over this a few months ago. I have been persuaded that it's not that hard to do. Yes, there is an authentication issue. Yes, a lot of people who have set themselves up as private sector, cyber security folks don't have the same rights that law enforcement do, but that doesn't mean they couldn't be somehow accredited and provided access to the data just like a university researcher can go to a university research protocol and get the data.

We don't need to imply that we are shutting these things down forever. That goes with the whole determination of purpose and whether you meet the requirements. And the requirements could be all kinds of things, accreditation as a cyber security organization or, you know, one thing or another. We seem to keep dancing around that.

And people get fairly shrill about losing access. That this has been a legal and we need to fix it. So I think we should get on with figuring out what that tiered access looks like. Thanks.

Chuck Gomes: Thank you, Stephanie. This is Chuck again. Don't mute yourself yet. But I would like to ask, so if I'm understanding you correctly, you'd think it would help us in the things we've been trying to do the last few months, if we got two gated access or differentiated access sooner. Am I hearing you correctly?

Stephanie Perrin: I do think that we might - this is Stephanie again - that we might stop going in circles. And I'm guilty of driving us in circles because I'm going to identify every - what Greg described as a gotcha, as we go along and we try to pick these things apart because I won't agree with it without 16 caveats that go without agreement just like I wouldn't agree to say gated access is okay unless you've set up all three conditions and the purposes and the situations under which you wouldn't release because that's just how it works, it's that complicated.

                 Did that clarify or further obfuscate?

Chuck Gomes: Yes, so thank you, no I think I understood you correctly (unintelligible). Let's go to F, personal data is not or cannot be publicly published. I think the data protection experts that we received answers from believe that. Pretty clear on what they said. They criticized over and over again the fact that - and letters that have been given to ICANN the Corporation, and the one I read today, you know, they keep criticizing the same thing, that there's just all this information that's publicly published, and for personal data that should not happen is what they say.

                 So I think certainly we can conclude that the data protection experts that we asked questions of support this statement so like that. Now, certainly if somebody wants to comment on this I'll allow a couple of minutes. But I want to go from here, and we're not going to go to the third question because it's going to be even tougher than the one we are working on, and we have limited time.

I would like for us to go to Question Number 2, in other words the first question in the poll, other than your name, and talk about that one a little bit while we have some time. So anybody want to comment on F?

And I apologize, trying to stay on top of what everybody is saying and managing the queue, I have done a terrible job today of staying up with the chat so please accept my apologies for that. And again I always ask for people to jump in and referred to comments in the chat so that when I miss them, which I will often, somebody can point them out.

Okay, let's go then back up to Question Number 2, if you'll scroll up to Question Number 2 towards the beginning here. And you can see the results of there. The interesting thing when you look at the results there, even though there was one person who disagreed, and that person didn't comment so if that person is on the call they're certainly able to comments now.

That even the others didn't really seem to be disagreeing. There's just a lack of clarity in terms of the wording. And several people had trouble with the way this was worded. And we actually came up with - I think - what was it, the fourth comment I think actually suggested a wording that might be kind of helpful. And, Lisa, or Amr, do we have that wording that we can maybe put in the notes or in the chat, chat is fine, we can do it in the chat.

I think it was Comment Number 4, so you may want to - if you scroll down a little bit from the question if you look at Comment 4 there, it starts off, I missed the point, but to me it looks like - and the part that seems helpful is every legitimate purpose requires a domain name, there's probably other ways to say that. And I think in the leadership call we came up with a variation of that that's almost like that. Lisa, can that be put in the chat or the - go ahead, Lisa.

Lisa Phifer: This is Lisa Phifer for the record. Yes, that's in chat there. We took that exact wording but in keeping with our discussion from last week appended as a

registration data element, I put that they're in chat, every legitimate purpose requires a domain name as a registration data element or every legitimate purpose requires a domain name registration data element.

Chuck Gomes: Okay, so you can see that in the chat there and Lisa's input there. What do you think about that statement? Is that one that we could accept for now? Anybody object to that statement - kind of re-statement of what was stated in Question Number 2? Marc, go ahead.

Marc Anderson: Thanks, Chuck. This is Marc Anderson for the record. Not an objection, just a reminder for everybody, I think Kal is mentioning post queries, he's getting along the lines of what I'm going to remind everybody today. In the existing Whois we have three types of lookups, we have domain name server and registrar lookups.

You know, so, you know, at least for today, the RDS, that would not be a true statement. Of course, you know, as everybody is aware, you know, we're free to redesign this as need be, so maybe we decide that tomorrow's RDS solution it is a true statement. But just to remind everybody that domain lookups aren't the only purpose of RDS today. Thank you.

Chuck Gomes: Thanks, Marc. That's helpful. Should we, I mean, maybe we should modify this a little bit to accommodate that. Anybody have a suggestion in that regard? Should we say requires a domain name, host or whatever registration data element? I see some people typing so we'll watch it there. Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I think the question isn't whether there are other data elements that might also be needed but whether this data element is needed.

Chuck Gomes: Jim, go ahead.

Jim Galvin: Thank you Chuck. Jim Galvin for the transcript. I guess I'm being a bit confused here by your question, and maybe the context in which Marc was making his comment. Again, I want to dry distinction here between collection and publication. It seems to me that the reason why we're here is because of domain names. You know, everything else is kind of ancillary to that, just to state it in the extreme.

And so maybe that's the point that we should talk about a bit as to whether or not that's true. I mean, in that context, you know, the domain name is sort of the obvious principal identifier, if you will, or principal index element if you will. It seems to me that if you don't have it and it's not part of your collection then, you know, I don't even know why we're here.

To more directly respond to the comment about other kinds of queries, what Kal was saying in the chat, and I think Marc was bringing up also, you know, that's a publication issue. That's called how do we want to provide access, you know, given that a stated legitimate purpose in what way are we going to support our ability to do things with that data, access it, you know, massage it, analyze it, whatever that might be.

And I think that that's a separate question that will come up later. You know, whether I can query the RDS based on a registrar ID or name or, you know, name of registrant or query things based on domain name. Again I want to emphasize those are publication issues. We will get to those later when we talk about how we are going to provide that service, if at all, and on what, you know, authoritative or legitimate grounds we might do that. Thank you.

Chuck Gomes: Thanks, Jim. Anybody else want to comment on that? Thanks, Kal and Marc for your comments there. I'm not sure if there's a quick resolution on this or not; there may not be. I think Jim's basically right that - and of course the name of the DNS, the Domain Name System, the domain name certainly is a key element even though it is not needed, as Kal says in the chat.

You don't have to even think of a domain name to search for a registrar or a name server. So that is certainly accurate. So maybe we need to give this some more thought in terms of a concluding statement. And I see Lisa's typing there.

One of the things that - and first of all, let me make some general comments about today's meeting because I don't know if the rest of you see it this way or not but it seems to me that this discussion we've had in this meeting is really a good picture of what we have in front of us and what we have to do and what we are trying to do.

And it's not an easy task. But several people have pointed out that, you know, we're not trying to exclude anybody and their needs that are legal and legitimate purposes. But a lot of our purposes conflict with laws and with other people's purposes. And so what we have to do is to try to find a way, and that EWG report fortunately for us, I mean, they worked countless hours and months to come up with some ideas that give us ways that we might be able to address our competing needs. And I hope all of us will think constructively. And please don't be afraid that we are going to ignore - if your needs are legitimate by the community standards, we are not going to ignore those things. We've got to find ways to accommodate all of them, and you can't just do it straightforward because you will step on some people's toes, if you do that.

So it is a challenging task. But this call I think has really illustrated what we have in front of us, and so my first caution, and I said this I think last week or the week before, try not to be fearful that your issues are going to be addressed. We really are going to work hard to address all of the legitimate needs. It's not going to be easy because one person's needs goes against somebody else's, and so how do we accommodate both? And that's what our goal is.

And again, the EWG report did an awful lot of work to make our job easier. And let's take advantage of that. It doesn't mean we have to accept that all as fact, but it really is a lot of good work. And it provides solutions that we may be able to apply to meet our competing needs. So again, if you haven't looked at that recently go back and look at all the work they did. That didn't happen overnight, it happened over not only tons of hours by the working group but several comment periods and lots of input from the community and so forth. So please remember that.

Okay, I'm not sure we can do too much else on Question Number 2, were not going to cover Question Number 3 today so there we have enough time for wrap up, at least a brief wrap up in terms of that. We really - we should take a quick look at Agenda Item 4 on the - you can go back on the notes to the beginning to see the agenda if you need to.

But it says, I'll read it, continue deliberation on the charter question, sub question 3.1, which has been rephrased. "What are the purposes of each existing gTLD thin registration data element? Do they sufficiently meet the needs of purposes identified as legitimate?" And there was a merge, thin data purpose document that you have a link in the agenda if you want to look at that. We're not going to have time to delve into that, and in doing that that's how we got into this whole question of authoritative that's being worked on.

And last week we talked about the issue of minimalist data was talked about and so forth, so those are things we will probably have to talk about further as we go forward. The - and with regard to the European data protection experts, again, that's not all we're going to look at in terms of, not just their interpretation of the law and so forth, but at some point we are going to have to decide what parts of that law will impact a portion of our community in Europe and in other jurisdictions?

And what other regulations will impact people from different jurisdictions because we can't create our requirements and ultimately policy without being

aware of those things. So at some point we are going to have to find out okay, what are the accepted interpretations of the global data protection requirements that are going in the place in Europe? And what other jurisdictions in the world may have similar ones?

So, we do need to reach some sort of - some conclusions with regard to the answers to the questions that we got. And we will continue going through those. I'm not sure what the best way is to go through those and to pull out things that we need to confirm, things that we can agree on and so forth. There seem to be quite a bit of agreement tonight that we're going to have to look at this idea of personal individuals versus non personal and it's not just a matter of somebody being incorporated or whatever because there are individuals who operate businesses as individuals and never do any incorporation so it does get complicated.

So if any - as we close here I'm curious, does anyone in the working group have any suggestions as to how we might most effectively go through the answers and solicit answers from people who weren't one of these data protection experts without dragging this thing on forever. There is lots of information that they've given us and we are going to have to react to it one way or another and probably come to some compromise positions.

Anybody have any suggestions in terms of how best to proceed through all 19 questions, not just Question Number 2? I don't know whether we will have a poll this week or not. If we do, it may be just a question - some things like we did on Questions 3 and 4 to help just motivate all of you to start thinking - looking at some of the answers and that - I haven't talked to the leadership team about that so you will see it if there is a poll, if there isn't we'll let you know one way or the other.

Stephanie, go ahead. Are you on mute, Stephanie? We're not hearing anything.

Stephanie Perrin: Can you hear me now?

Chuck Gomes: Yes.

Stephanie Perrin: Sorry, the line dropped apparently. Stephanie Perrin for the record. I would suggest, and this is one of the reasons I didn't complete, that those were nit-picky questions that we asked in some cases, some were broad but some others were very pointed questions. And some of the answers require unpacking. So I think they don't really lend themselves to being picked apart and placed into polls.

I think we really, as painful as going through all 19 questions might be, I think we need to walk through them and make sure that people understand what the answers mean. I think we could easily do six or eight a night. And I think we kind of owe it to the data commissioners, since they took the time to go through our questions, we kind of owe it to them to go through their answers.

I'm a little reluctant to just try and pick them apart and throw them into a poll and see what people think all by themselves particularly if they don't necessarily understand the context of the question. Thanks.

Chuck Gomes: Thank you, Stephanie. This is Chuck. So what you're suggesting is that we go through them as they - each answer as a whole and discuss it in our working group meetings and do several each week and let people ask their questions, let people poke holes if they think they see holes, let other people defend, whatever the case may be, so that if nothing else we have a reasonable assurance that we are understanding what they were saying, whether we agree with it or not? Is that kind of what you're saying, Stephanie?

Stephanie Perrin: Yes, that's basically what I'm saying. Some of them might be quick, but some of them, judging from the circles we go in, might take a while. Thanks.

Chuck Gomes: Yes, okay. All right well thanks. I asked for suggestions and much appreciated. Well, our time is up. Maybe we're a little over, it looks like. So I need to wrap this up. Lisa, or any of the other - of the vice chairs, is there anything that we need to cover other than the next steps and the next meeting? The next meeting of course will be at our regular time next week, you can see that in the notes on the 25th at 1600 UTC. And we will continue going through the answers to the questions and we'll try to get to our - looking at purposes for thin data elements. So is there anything that I have left out?

Okay, well thanks. I personally think it was a really good discussion tonight. We didn't get - I don't know that we resolved anything but hopefully we're understanding each other and our needs better, and building respect for one another and our differing viewpoints so that we can work together to find solutions. With that said, thank you all and have a good rest of the week. The meeting is adjourned and the recording can stop.

                END