ICANN
Transcription
Next-Gen RDS PDP Working group call
Tuesday, 9 January 2018 at 17:00 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: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-09jan18-en.mp3

AC recording: https://participate.icann.org/p7tsynp7hxi/

Attendance is located on wiki agenda page: https://community.icann.org/x/QgByB

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 started.

Julie: Thank you very much. Well good morning, good afternoon and good evening everyone. Welcome to the Next Generation RDS PDP Working Group call on the 9th of January, 2018. In the interest of time, there will be no roll call. Attendance will be taken via the Adobe Connect room. If you're only on the audio bridge would you please let yourself be known now? Okay, hearing no names I would like to remind all to please state your name before speaking for transcription purposes and to please keep your phones and microphones on mute when not speaking to avoid any background noise.

And with this I’ll turn it back over to our chair, Chuck Gomes. Thank you.

Chuck Gomes: Thanks, Julie. And let me start off by saying happy New Year to everyone. Hope you got a little time off over the holidays and some rest. Certainly I hope you got some – a little break from the working group. I am currently in a RV park in Tucson, Arizona near an Air Force base and an airport so if there’s a little bit of background noise from airplanes, sorry about that. So I have all the windows shut so hopefully it’ll be muted a little bit.

Thanks for participating in the survey before we took the break. And during the break somewhat, we'll be going over that a little bit later. You can see the agenda in Adobe. Let me ask if anyone has an update to their statement of interest. Okay, not seeing – oh I see a hand. Greg, go ahead.

Greg Shatan: Hi, this is Greg Shatan for the record. A couple of update to my statement of interest. First I've joined the law firm of Moses and Singer as a partner in New York so that's a new employer. And secondly, I've joined the Board of Directors of ISOC New York and also am serving as the alternative representative of ISOC New York to NARALO so that's an addition to my ICANN world. Thank you.

Chuck Gomes: Thanks, Greg, very much. Anyone else? Okay, then let's jump right into the agenda. We'll bring up the slides for today's meeting; hopefully you had a chance to look at those. And we'll proceed right into agenda item Number 2, just briefly, to complete our deliberation on data required for domain name management, so if you scroll down to Slide 3, we'll just spend a minute or two on that. We're not going to re-deliberate any of this.

But there were – there was 92% support in the last poll for the agreement that you see there that says, "The following registration data is needed for the purpose of domain name management: domain name, registrant name, registrant organization, registrant email, registrar name, creation date, updated date, expiration date, name servers, domain status, and administrative contact."

Now, let me point out that there were some really good comments submitted, some that suggested other data elements. Okay, you can see in the third main bullet item there, there are four responses in particular that gave rationale for adding data not included in that list such as the registrant postal address and phone and technical contact.

Now there wasn’t enough support in the overall working group in our meetings and on the list to add those but I encourage those who believe they should be added to watch as things proceed and when we start wrapping things up in terms of purposes for collection, if you still think it’s an issue of course we can discuss it again and you can try and convince the rest of the group. But again, thanks for those comments. They were not ignored, in fact the leadership team talked about them quite a bit.

So what we're going to do is accept rough consensus on that agreement, so that’ll be added to our list. And one of the things, just to let you know, I don't think it’s available today but staff is going to create a list of all of the working group agreements where we have – had rough consensus that collection of certain data elements is justified for certain purposes and those will be summarized in a table format so we can kind of all keep track easily of where we're at.

Going then onto Slide 4, and what we want to do next is complete deliberation on domain certification as a purpose. In the poll results 84% supported the working group agreement that you see on the screen that domain name certification is not a legitimate purpose for requiring collection of registration data but may be a legitimate purpose for using some data collected for other purposes, keeping in mind that access requirements will be deliberated at a later stage.

Three responses proposed revisions to that text and we’re going to look in particular at those comments but we can look at other comments as well. So if you will scroll to Slide 4 – or excuse me, Slide 5, I was on Slide 4 I think, yes, Slide 5, sorry, I was off on my numbering – you'll see the six comments, okay, Comments 4, 5 and 6 we definitely want to maybe spend a little time on if the working group does, but we can talk about the others as well.

So there was some good discussion on the email list and I confess that because I was busy doing other things I was current on email up to about an hour and a half ago but I'm not current and there's been a lot of email since then so if somebody wants to bring up something that was in a more recent email feel free to do that, especially right now as we're talking about domain name certification as a purpose. Okay?

So I'm just looking real quick in terms of – I don't think I see Brian Winterfeldt. Rod is on. Let's see, Rob Golding is not. And Maxim is driving so he maybe mostly listening. But let me throw it open to Rod, since you submitted one of those comments that we're calling attention to today, and see if you'd like to say something. And then after you jump in I'll call on Greg. Rod, are you on mute? There we go, I think I hear something.

Rod Rasmussen: Yes, I'm trying to – can you hear me now?

Chuck Gomes: Yes.

Rod Rasmussen: Okay, sorry, now I'm trying to find my hands-free device. I'm having some noise on my computer, so which usually isn't very good. So Rod Rasmussen here. So, yes, just my comment on this was that this is around the fact that not everybody who wants a domain name or has a domain name will have to cert so from a collection standpoint it's not required but – you have to enable it if you want to enable – you know, if somebody does want a cert tied to it.

So that's why I – kind of the fact that needs to be – it needs to be – it needs to be covered in some fashion as an option rather than a requirement, but if you are – so, you know, how you want to define that from a – an overall perspective is I guess up in the air, but, you know, it is not a requirement for everybody who has a domain name to provide information in order for certs – cert operations.

However, if you do want a cert than it is, you know, that information and we could have a discussion about that, is required right now. So the – might be splitting hairs but I think it's important that we be precise about what circumstances it is required and what is isn't, but from a collection perspective in general it's not; from a collection perspective if you want to use a cert in conjunction with your domain name it is likely required. J

Chuck Gomes: Thanks, Rod, that's appreciated. Greg, go ahead. Greg Shatan.

Greg Shatan: This is Greg Shatan for the record. And this harks back to a discussion we've had at least once before about what is meant by "required." And I would use – and I think we should use the word "required" a little differently than Rod is using it. Rod is using it in the sense that if it's always necessary can't live without it, it's oxygen, then it's required. It's only required some of the time it's not required. I would put it the other way, which is that if it is required some of the time or for some users then it is required. Universal requirement is a very high bar. But if it's required for some sectors, for some activities, for some certification, then it's required for a certification.

And I think that's – we need to kind of have a consistent use of the term "required" or else we're just going to end up with a muddle and make it very difficult to create policy much less implementation. So I would – based on what Rod himself said, I would say that it is required.

Secondly, I'm sorry that I did not participate in the poll but, you know, if I had I would have disagreed with the proposition that domain name certification is not a legitimate purpose for requiring collection. I think again this goes to the issue of what is the purpose of Whois/RDS? And some people seem to think that the purpose – main purpose is to facilitate registrant, registrar relationships and to provide the information necessary for that.

That to me seems to be information that's used but – and maybe the same as RDS Whois information but not the case; you don't need to have any Whois at all for you and your registrar and the registry ultimately to have a source of information amongst the three of you. The essence really of Whois and RDS is third party use and use by, you know, and I'm counting certification authorities as third parties.

And if there's significant disagreement on that point, then I think we have another kind of fundamental issue that we need to straighten out as to what it is that we're working on in the first place. So that's my two cents. Thanks. And…

((Crosstalk))

Chuck Gomes: Thanks, Greg.

Greg Shatan: …against the agreement.

Chuck Gomes: Yes, okay. I have a couple follow ups with you. First of all, I personally agree with your logic in terms of "required." But my follow up question to you, why would it be required to be collected for the RDS? Keeping in mind ICANN's mission and that is elements of that are attached in this presentation if people want to scroll forward to that.

What part of ICANN's mission do you think relates to – and I understand that some certificate authorities require a domain name, some don't. And there was some disagreement on the list on that and that was healthy. But what – on what basis would it be required for the RDS? Not talking about requiring it for a certificate. Greg Shatan, you can have the floor again if you want to respond to that.

Greg Shatan: Yes, well I would say that the – and I'm not exactly sure the question you're asking – I thought until the last thing you said that the question was why would information collection for certificate – for use by certificate authorities be a requirement? And my answer to that would be, under ICANN's mission is that this goes to poor issues of security and trust which are key to ICANN's mission. So I think that's the question you were asking.

Chuck Gomes: It is.

Greg Shatan: But if it’s not then maybe you can rephrase.

Chuck Gomes: No, that’s fine. I appreciate the response. Let’s go to David.

David Cake: Thanks. I mean, I’m just looking at (unintelligible)…

Chuck Gomes: David, you – we heard you for a little bit and then you cut off.

David Cake: Sorry, I think that somehow muted me. I agree with what Greg said about the use of “required.” I think we do need to be clearer on what is meant by “required.” The quoted – the two examples both I think are not really addressing the issue that we discussed on the mailing list today. There is a process for validation of domain authorization and control that uses the RDS but it’s one of multiple processes that you can use to validate domain authorization control.

So the fact that there is one possible process that uses it, which is optional and there are – which there are easy alternatives and in fact the easy alternatives are regular use – you know, more common use. So that – whether or not, you know, there is a process that uses it, that there are easy alternatives to that you don't have to I don't think that justifies requiring – it is a requirement. And the other example from Legit Script seems to be talking about an entirely different – almost completely unrelated use of the term “certification.”

It’s been an application to our current sort of discussion, seems to be sort of circular in application, so, yes, I mean, I agree with the use of the requirement, I just think any of the specific objections that have been raised really change the idea of – raise enough of an objection to show that it is in fact required even considering what we mean by whether or not you – I mean, my point is I'm agreeing with Greg but if we said, well, you know, if you need to use the RDS data to get a domain name certificate, that would be a real issue, but we clearly – that is not the case.

I mean, I'm disagreeing with Rod there, I don't think there is any case in which you need to use the RDS in order to obtain a domain name certificate and in fact there are alternatives to every use. So and for most data you are positively discouraged, you know, you're told – literally told not to use that data. So you know, in the general case I agree with Greg, in the practical case I disagree that we – that any of these specifics constitute requirement. Thanks.

Chuck Gomes: Thanks, David. Let's go to Andrew.

Andrew Sullivan: Thanks. It's Andrew Sullivan here. I guess I'm having a little bit of trouble with the question, Chuck, that you posed which is, "Is this required for the RDS?" There is nothing required for the RDS, right? We could get rid of the – at least the publication thing of this because it's an instrument for other purposes. So the question I think that you maybe were trying to ask is whether this is necessary to support the operation of the Internet ecosystem that depends on domain names.

And I think the answer to that is it is not precisely required, for exactly the reasons that David just outlined, but it is one way that this system works. And I think when we talked about this last time what Rod was trying to propose was a – was a modification of this that said, it is not a legitimate purpose for requiring collection but a registrant may provide it and a registry may collect it for this purpose. The objection here I think that people are raising is the idea that you're using the data collected for other purposes.

And it's possible that a registrant might provide this information for this purpose; might provide some information to the RDS for the purpose of supporting a certificate authority in its examination. It is not okay for the registry to require it for those cases but it’s still a legitimate reason to collect the data with informed consent on the part of the party who is providing the data. And I think that that is the way that we talked about this before.

I will say that I am prepared to accept it for – accept this agreement anyway the way it’s worded, just because somebody could gin up some other reason to collect the data and, you know, and come up with it and then provide it to the – to the certificate authorities, that way. You know, you're not actually even going to be able to tell what the intention of the parties involved is so I don't really care. But as a practical – or as a strict matter, it does seem to me that we have agreement that if the registrant agrees to provide the data under those circumstances then by definition that is a legitimate purpose for collecting the data, it’s just not a legitimate purpose for requiring that collection. Thanks.

Chuck Gomes: Thanks, Andrew. This is Chuck again. And before I go to Alan, let me back up a little bit. By the way, I’m fine, Andrew, with your reformulation of my question. That’s fine. But keep in mind what we’re doing in Phase 1 of the working group is developing a list of requirements that would be needed either on a modification to the existing Whois system, or on a new system, okay?

And at the present time, we’re developing a list of purposes for which we think some data must be collected and then we're going a step further and identifying data elements that must be collected for whatever this new system is or modification of the Whois system.

So keep that in mind in using the word “requirements,” that’s our overall task for Phase 1 is to develop requirements. And so we’re coming up with this list of domain name elements that must be collected, so they're required, in whatever system we end up with and recommend. And then some things we’re – we’ve made conclusions and one possible conclusion that we’re considering right now is that domain name certification there are no data elements that are musts for that as far as our work. I understand that nothing is totally required.

But keep in mind our overall task of developing requirements and what we're doing here. That said, let me go to Alan.

Alan Greenberg: Thank you very much. Andrew and Greg covered a lot of what I was going to say and probably better than I would have said it. As Greg pointed out, trust in the DNS is one of the reasons that ICANN exists. There may well be other ways other than certification to verify that a domain is owned by who you think it is so you can trust it. But we're not here to redesign the Internet and to redesign the mechanisms. Certificates are a major part of the reality of the Internet as it is right now and we must have an RDS which can support it. And if this information is not available through the RDS how else is one going to find out who claims to own a given domain name so that it can be certified?

So I think we have to work within the constructs we have and if there is no other viable alternative to doing it, then the RDS is where it has to reside. So I don't want to get into the semantics of whether is required or voluntarily given because this is going to be a use of it, and you're going to want certification, but regardless it has to end up being there and accessible to the right parties. Thank you.

Chuck Gomes: Thank you, Alan. Any other comments on this or on any of the comments either shown on Slide 5 or discussed on the list the last few days? David, go ahead. David, we're not hearing anything. It looks like you're off mute but we're still not hearing anything. Still nothing. Okay, all right so let's – I'll come back to you, David. Stephanie, your turn.

Stephanie Perrin: Thanks, Chuck. I hope you can hear me.

Chuck Gomes: I can.

Stephanie Perrin: Good. Stephanie Perrin for the record. I hate to start the New Year with a comment on how we maintain a failure to communicate based on the frame of reference of which we – from which we come. But this whole issue of whether this is a requirement is rather fundamental. So in a sense – while I accept Alan's logic in – with respect to how the data is required to enable certificates, and certificates are a good thing, and it may or may not be as Jim points out in the chat, ICANN's business to be enabling, facilitating and required – and providing the data required to enable secure certificates, my point is simply that if you don't need a certificate, you should not be required to provide data that is not – I hate to use it again – required for your purpose.

In other words, does registration automatically mean that you must embrace every possible next use of the data? Thanks. Obviously, as I pointed out in the chat, this is the antithesis of data minimization from a data protection perspective. Thanks.

Chuck Gomes: Thank you, Stephanie. David, did you get audio back? So if I can go back, hopefully David can get audio, if we can – and you can see that staff is trying to troubleshoot that. If I go back to Greg's – Greg Shatan's logic and kind of follow up maybe a little bit what Stephanie is saying, so if we – if every possible use – if we have to collect a data element if there's one legitimate use in the global domain, I guess we'd collect everything. We know that's not going to fly with regard to at least legislation in Europe.

But we have to at this point at least come up with a – something. If there are data elements that must be collected for domain certification for the RDS, then we need to identify those. Right now our tentative conclusion is that, as you can see at the bottom of Slide 5, that it's not a legitimate purpose for collection of any registration data. But we're acknowledging that it may be a legitimate purpose for using some data collected for other purposes. And as Stephanie points out, the fact that – if we come to this conclusion that doesn't mean that the system, whatever it is, couldn't allow for optional input of data that's need for certs. And of course that would have to be coordinated with registrars and so forth. But that's a doable thing.

But I think Stephanie's right that requiring someone who doesn't have any interest in getting a certificate to provide data – keep in mind when we're saying "required to be collected" it would be collected of everybody. That doesn't rule out the option of providing some optional elements, and registrars already do this in their registration processes that people could provide. So keep in mind though what we're focusing on is required collection of everybody who has a domain name. David, did you have any success? If not, maybe you can – you can put something in the chat. I'll pause to see if David – not hearing anything.

Let's go back to Andrew.

Andrew Sullivan: Hi, it's Andrew Sullivan here again. Chuck, I'm a little concerned about the way you just described what we're doing here because my concern has been all along this term "legitimate purpose" which it seemed to me was a critical thing that the earlier briefings that I understood or to the extent that I understood them anyway, said that was a critical part of this. And the point that I've been trying to make is that these may be optional elements but if this is the only purpose for their collection it's still a legitimate purpose.

So it's not a legitimate purpose for requiring this collection, but it is a legitimate purpose for the collection of it. And that's the difficulty that I think Rod has been trying to fix in this agreement – in this proposed agreement proposition. Thanks.

Chuck Gomes: So thanks, Rod. That was helpful for me I think. Maybe what we need is – and I'll just throw this out because I haven't mentioned it to anybody before, but maybe what we need is a couple different statements here. One, as stated in the box at the bottom of Slide 5 but another one that it states it's a legitimate purpose for – I don't know how to word it – optional collection or whatever, and would that resolve the differences that we seem to be dealing with? And I'll leave that there for a minute. And I see that Lisa put something from Rod in the chat so let me glance at that a minute and then I'll turn it over to Greg Shatan. In fact I'll turn it over to Greg and I'll read what Lisa put in the chat there in responding to Rod. Go ahead, Greg.

Greg Shatan: Thanks, Chuck. And I think the way you phrased the requirement at the end of your last prior intervention gave me some pause. You said that we were only considering required something that is required of – for every registrant. And that's, again, I think going against my idea of what required should mean. But rather than trying to parse the word "required" one way or the other, maybe we need to have two categories at least for this point which is things that are always required and things that are sometimes required.

If you are a registrant who wants a certificate, and, you know, many, many, many registrants do – can't do without them, then this is mandatory information and I would assert it is a legitimate purpose for collecting it based on ICANN's mission and on the intended use of RDS information generally. But rather than trying to argue whether required only means always necessary or also means sometimes necessary can be avoided at this point by using both terms and maybe we can have a more confined discussion of what to do with things that are sometimes necessary.

Maybe there's an opt out. If you, for instance, are a registrant who will not want a certificate, and there is no reason to collect that information from you, and you opt out of having a certificate and until some – until such time as there is an alternate reality in which no – there's no requirement for any of this information for any certificate, you know, you're just not going to be able to get a certificate or if you do you're going to have to revise your Whois and opt in to the information and provide it.

You know, so that may be getting down into implementation level but I think it also shows why sometimes required really is required. Thanks.

Chuck Gomes: And I was – thanks, Greg. And I was of course focusing on one of the things I said on what is really required whereas several of you have pointed out there are some things that aren't required of everyone but they're allowable for collection. Everybody look at Rod’s latest formulation. And I think Lisa responded to that in the chat. And see if that helps resolve the issue that we're talking about? Keeping in mind that I think Jim pointed this out a long time ago in the chat, that ICANN’s not in the certificate business, it’s not part of their mission, okay?

Nor is the RDS, I don't think, intended to meet every third party need that exists. But if we as a working group make a recommendation that certain purposes are – and I’ll use the term “legitimate” for collection or maybe just access, we can make those recommendations, that’s what our job is. And the first thing is to establish the requirements.

Now let’s talk about the reformulation of this possible working group agreement. And because it’s changing – we don't like to go back and re-poll but we may have to on – in this case. But let’s listen to some other people. David, did you ever get audio? You can speak if you did. Go ahead and try.

David Cake: Can you hear me now?

Chuck Gomes: Yes. Welcome.

David Cake: Okay, this is a very confusing delay. But what I’m trying to say here is that (unintelligible) about, you know, until such time that it’s not required to use the RDS collecting any data for the RDS to get a certificate, Greg, that time is now. We can easily get a certificate without any use of the RDS including high level certificate, extended validation certificate. That’s all. Thanks.

Chuck Gomes: Thanks, David. Stephanie, go ahead.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. I think Lisa has very succinctly reminded us of the task that we are doing and unfortunately for progress every time we stray into things like mandatory and required for everybody, that gets us into later evolutions of what this group is trying to develop. And some of us are hoping for a much more complex celebrated system that looks after the principle of proportionality which is what is thrown out the window when you require everybody to provide data for some purposes.

But what – the reason I put my hand up – and I would point everybody to what Lisa summarized there, the reason I put my hand up was possibly it would be useful to come up with an example from another field that might help clarify (unintelligible) to. My bank wants information about me. It has a minimum data set that is required for a savings account; minimum data set for a checking account. And then it wants more data partly because the banking field is regulated and it has to get this data, if I have an investment account with them.

Now, they want that investment data from the get-go because they want to sell me RSPs. That doesn't mean that I'm, A, required to give it to them, or, B, that I want to, you know, unless you trust everybody which that's a whole other discussion, why would you do this? So that's the principle that we should be thinking of when we're building the RDS. Yes, it's mandatory for certain purposes and maybe the time to make that distinction is now. I agree with what Andrew said, it's one of the fundamental problems with the way we (word smith) and I don't see a better way. It's inherently convoluted, but we keep running up against this wall. Thanks.

Chuck Gomes: Thanks, Stephanie. David again.

David Cake: Yes, just to go back to Greg's – replying to Greg in the chat which is really – that when it say it is possible to get a certificate without any RDS info, I mean, it is not – RDS info is not required for any certificate unless…

Chuck Gomes: A little louder, David.

((Crosstalk))

David Cake: …RDS is not required to get any certificate unless you have a particularly inflexible certificate provider that refuses to use the alternative methods available in which case you should go to a different certificate provider who will I'm sure quite happily use another method to validate your domain name control. That's all. I really – any of these arguments that say if we don't allow this, certificates won't be issued and it'll be terrible, even under some sort of – some particular type of certificate or similar it really – I don't understand how this argument persists. That's all. Thanks.

Chuck Gomes: Thanks, David. Greg Shatan.

Greg Shatan: Thanks. As I have noted before, we're not in the business of putting people out of business. If there are certificate providers that require RDS or Whois information then some certificates use them and therefore it's required. You know, so David, you kind of lost me at "unless." If it was just completely not required for any certificate from any provider then this would be a different discussion, but as long as it's required for some certificates by some providers, then it's required for certificate provision conceptually.

And that's where we're at. We have to – the idea of this is to enable, unless we want to disable certain businesses or business models we have to enable them as they've decided to function and we don't know if they're particularly inflexible or want to be particularly accurate or what their reasoning is, until we get a certificate provider here who can discuss with us why they do or do not or how they do or do not use Whois or RDS information, I think we're all, you know, somewhat grasping at straws. And the last thing I want to do is try to guess at their internal reasoning and whether it's good or not or inflexible or not. Thanks.

Chuck Gomes: Thanks. Thanks, Greg. I want to call attention while going to Alex, everybody take a look at the – at alternative in chat that seems to be getting some support in chat at least. And we will – we'll come back to that. But Alex hasn't jumped on this yet so welcome your contributions, Alex.

Alex Deacon: Thanks, Chuck. This is Alex Deacon for the record. I was going to start out by saying that I think Rod's original suggestion, wording in Point Number 4, I think makes more sense, but looking at what Lisa has put in the chat I think I'm with others, that may be also do the trick. But I'm also a little bit concerned that specifying that domain name certification is not a legitimate purpose made by this later on, and I think this is the point that Maxim was making in his Comment Number 6. Hopefully not but I just wanted to kind of highlight that concern to make sure that, you know, we don't agree to a formulation that may be useless down the line or may – or may kind of be – or data protection officers may object to with regard to use in the future.

And then I'm wondering if it makes sense to invite someone from the domain name certification business? I know we used to have people from Symantec, now DigiCert, on the group, I think they've since left. I'm not too sure any of us here are – can call ourselves experts of the current industry. And it may help just to kind of get a concrete understanding from people in the business of exactly how and when and if they use data from the RDS just to make sure we're not making any assumptions or incorrect assumptions with regard to how the business runs today. Thanks.

Chuck Gomes: Thank you, Alex. Alan, you're next.

Alan Greenberg: Thank you very much. I think we're largely agreeing here, and we're in a drafting mode. And I think using 100 people or 50 people on a phone call to drafting is a particularly ineffective way of doing things. I think there is general agreement that domain name certification is legitimate purpose for the collection of registration data, but not a required one for everyone. If we are agreeing with that can we assign someone to go off and, you know, give us three different versions and then we can vote on which one we like best or something instead of trying to continually refine the drafting as we're talking her?

Chuck Gomes: Alan, what's wrong with…

((Crosstalk))

Chuck Gomes: …the latest one that Lisa put into the chat?

Alan Greenberg: Sorry?

Chuck Gomes: What's wrong with the one – the latest one that Lisa put in the chat?

Alan Greenberg: I'm not disagreeing with it, I'm saying I think – and several of these would be quite viable, but I think continuing the discussion if it's going to continue, if it isn't going to end now, is not a viable way of using the time. That's all I was saying.

Chuck Gomes: So the leadership team is in agreement with you. We try to avoid drafting on the calls. But going back and putting – having somebody do three and then polling on those and discussing those, if we do that on every one of these things again we'll be here for 10 years. I won't be but the – so I'm not too inclined to go that direction.

Alan Greenberg: Yes, my – Chuck.

((Crosstalk))

Alan Greenberg: Chuck, if I may? My point was we spent the last 30 minutes where I think we are largely agreeing on the concept.

Chuck Gomes: Agreed.

Alan Greenberg: And that's the problem.

((Crosstalk))

Chuck Gomes: Okay, point made. Okay. The – so using what's in – what Lisa put in the chat there including Steve's suggestion there, domain certification is not a legitimate purpose for requiring collection of registration data but may be a legitimate purpose for allowing some data to be collected or for using some data collected for another purpose. Now, my suggestion is, is that – and my leadership team members are liable to shoot me if they could reach Tucson where I'm at because we don't like to re-poll, but I don't see any way to avoid re-poling on that reformulation because I think quite a few people that had concerns and some didn't participate in the poll and that's understandable.

Are there any – are there any serious objections to re-polling with the new formulation? And Lisa and others, if you – you can object too because I know we try to avoid that but I'm having trouble seeing how we avoid that here. Please speak up if you have a serious objection to that and then we'll wrap up Slide 5 for now, okay? And there will be a poll question with the new formulation and some background given for those that aren't on the call. Okay?

All right, David, is that a new hand? So we still didn't make Greg happy, not terribly surprising but hopefully he'll let us know why. If you expressed it, I didn't get it.

David Cake: That was a – I just – sorry, I thought I'd keep that hand just to make one comment that I'm just trying to type in…

((Crosstalk))

Chuck Gomes: Okay go ahead.

David Cake: …just to clarify – it was just to clarify that if we are going to talk about which – that there being an optional case for collection of data elements to support domain names verification, we should probably mention which data elements we would be talking about and the only ones I can see are really domain contact data in that most of the information about sort of legal things appear to be required to verify by other means. That's what I can see, so basically the – because you can verify ownership via email from a domain contact is one of the sort of several optional methods that would seem to be the justification. Just clarifying what we mean by which data elements would be collected. Thanks.

Chuck Gomes: Thanks, David. I'm real leery of going down that path in cases where it's optional collection of defining which data elements would be optional. I think if it's optional and there's a need in certain cases that that'll be up to those who are collecting the data. If we try to define the optional level as well we may go 15 years.

All right, so let's go on to Slide 6 and we still have I think over that half hour. And we're going to switch over to another proposed purpose, criminal activity, DNS abuse. And just to set the stage, the drafting team, and we're going to hear from them in just a minute, that worked on this actually broke it down into three areas. We're going to focus on the area – one of those areas, investigation, there are two others that we will get to not this week but going forward. So we're breaking it down into three parts.

And keep in mind the Slide 6 is just a reminder of our approach – our building block approach. I'm not going to reread the elements of that but you can look at that if you'd like. Going to Slide 7 then, I'm going to turn it over to Rod. And it looks like Richard Leaning is not on the call. He was going to support Rod, but I'm going to turn it over to Rod who's agreed to give us a quick review. We're not going to go over this in full like we did many weeks ago. But Slide

7-10 kind of go over what this drafting team presented including notice on Slide 7 the three different areas. Again, we're going to start on investigation.

And rather than me continuing to talk, let me turn it over to Rod. And, Rod, just let people know when you go to – what slide you're on as you're sharing.

Rod Rasmussen: Okay, thank you Chuck. This is Rod Rasmussen. So I'm on Slide 7 which as Chuck already mentioned we've divided this purpose into three I guess sub purposes whatever word we're going to use for that – three very well related purposes, put it that way. And we're focused right now on this investigation perspective which is simply using the data to make some determinations around the nature of domain names in order to look at something that I have, as an operator in this space and look to find that in a second, has to – has in order to deal with an incident or something that's going on.

So next slide talks about the who, Slide 8, or actually the – yes, it talks about the who and the what kind of information is being used. And basically anything that's available because when you're investigating something you look for any of the clues you can use in order to make some sort of determination about what's actually happening.

The – I see Dick is on the call so in case I mess this up he can jump in. Anyways, the parties here are not just law enforcement or even, you know, cyber security folks but it's also other authorities that may be looking at things even IT administrators because a lot of people end up looking at logs are not trained cyber security folks, they're actually people dealing with wires, my systems being affected by this thing outside of me of my network.

And then there's a lot of automated systems that look at things and try and make some determinations around. And I'm not talking about the reputation side here, I'm just right now trying to talk about I've gotten an email message and I need to – it's hit the spam filters and I need to make a determination around what to do with that from a distribution perspective, thing like that.

Next slide, 9 is – and again it talks about the users and the various things that people do whether that's trying to determine whether a domain name was registered maliciously, whether it's to find additional things they're involved with, a particular incident or issue, or in order to form the process that you want to take to deal with an abuse issue, for example, I need to know whether or not a domain name is registered maliciously in order to know do I contact the registrar to have the domain suspended or if it's been compromised do I then try and find some information to track down somebody running a Website or owning a Website or owning a domain name or something like that in order to do the kind of contacting which is covered as a separate purpose.

I have to make a determination before I can go into that though to know who to best work with in that particular instance. And then if you want to move to Slide 10, and these are basically breaks things down into, you know, the nitty gritty of what you may need to be able to do in the distinct, you know, as from my description as you've heard, there's a lot of well you can do this, you can do that, you can – the idea here was to actually make that – make that concrete into the various more well defined kinds of issues and actions that people may use this information for.

And I'm not going to – we'll take the rest of the time if I want to explain that so I'm just going to, you know, that's there for people to refer back to. So I'm going to move down to Slide 11 which actually asks the question. Now – and then 11 and 12 basically do this asking of the question. And then if we move to 12 we come back to I think the bottom line as we talked about in Abu Dhabi, was that in general it's not necessary to collect any of this information in order to, you know, quote unquote facilitate an investigation of any sort. It's – the supposition here is the data is already collected and you're getting access to that data in order to do these various purposes.

And I think we discussed that fairly well along the way. But I think it's an important distinction here since we're talking about collection of data right now, you know, one could say, in a particular, you know, excuse me, a particular regime, that I'm going to collect all this data so that I'm – if you do anything bad then I have a record of who you are so I can track you down. I don't think we're at that level of domain names, what we do as investigators is take the data we have and use that.

Some of the data is extremely valuable but when we need to talk about that from an order of publication who gets rights to access that data rather than how it's collected because the assumption is, excuse me, I've got to cough again. And I muted there. There. The assumption is that enough data is being collected for other purposes, i.e., or e.g., establishing ownership, establishing the ability to transfer, all these other things that we're talking about that there will be useful information to support an investigation and, you know, the model we've had for 20 plus years has facilitated that.

So I would argue that if we fundamentally change the data that is collected, that this may change my thinking on whether or not this is required for collection. But as it currently stands, and as I think that we're leading to, the data will be somewhere, it's the matter of how you access it. And I think I can leave off there. Dick, did I leave anything out or are we good?

Chuck Gomes: Go ahead, Dick, feel free to either reinforce or add or anything you'd like to say would be helpful.

Richard Leaning: Yes, this is Dick. No, I mean, I echo what Rod said there. I'm just looking at the chat and my concern every time we talk about investigation, everyone's focus is on its law enforcement, it's law enforcement, it's law enforcement and everyone gets really nervous about law enforcement. And I just want to emphasize again is in this environment law enforcement, this is one of many, many, many other entities that are involved in investigation as was described when it comes to the Internet. In reality there is any abuse on the Internet, law enforcement is probably the last entity that people will go to to have a quick resolution of the issue. So I just want to – get that there.

And I've just seen Andrew Sullivan sort of agree, law enforcement is not the – is one of many people and I just want to focus on that before we get into real – into the weeds discussion about it. Cheers.

Chuck Gomes: Thanks a lot, Dick, I appreciate that. And thanks to both of you for being a part of that drafting team and for the whole drafting team and the work that they did. If you go back to Slide 10 you'll notice at the bottom there is an opportunity for anyone to ask questions about this particular purpose, not whether – let's not get into the questions that are covered on Slides 11 and 12 about whether some data should be collected or not for this, but rather understanding the investigation purpose related to criminal activity and DNS abuse.

So if anyone has any questions this is your opportunity to ask them. And we'll probably let Rod and Dick and anybody else who'd like to to respond to those questions. Okay. So there – all right, good. Thanks, Rod and thanks, Dick and the whole team for the work you did on that.

Going along to Slide 11 then, is criminal activity, DNS abuse, the investigation part of that, a legitimate purpose for collecting data? And the criteria and the tests are shown in Slide 11. I'll let you look at those on your own. You've seen those before but it's probably been a while.

And let's just open it up for a discussion. What do you think? You can see on Slide 12 a possible working group agreement. I would predict on this particular agreement we may have to do something like we did with certificates. And that's okay, okay, we probably don't have to repeat the same thing but we may need some modifications like we did with certificates that we can test in a poll.

But what are your thoughts on this? Again, just focusing on the investigation part of this purpose of criminal activity, DNS abuse. What do you think? Is there – do you think there's any data that – we're not going to get in data elements yet but is there some data that may need to be collected specifically for the investigation purpose or is it like Rod, and I think the drafting team ended up closely agreeing on was that the – its use of data that's collected for other purposes, it's okay to collect it for this purpose but not require it as we talked about with regard to certificates. Anybody want to jump into that discussion?

I'm assuming, David, that's an old hand. The – so I'm going to go to Stephanie.

Stephanie Perrin: Thanks, Chuck. Stephanie Perrin for the record. I think once again there's a distinct issue here regarding access to data. And I apologize, I'm sure I said this at our last face to face and I've probably said it before so I'll just be repetitive. But providing access to data that is collected for the purpose of registration of a domain name is perfectly fine to all of these parties be they law enforcement or other parties. Requiring data to be collected for the prevention of crime, the investigation of crime, any of these other things, you know, the establish of – establishment of reputation in order to prevent crime, all of these things, that is a serious expansion of ICANN's mandate in the view of those of us who are looking at basic due process rights.

In other words, it means that ICANN is in the business of collecting data about registration – registrants for the purpose of investigating crime, preventing abuse, establishing reputation to prevent abuse, all of those things. That is, I would suggest, outside its mandate. The business about the security and stability of the Internet does not involve investigating, collecting data, about individual registrants for that purpose. And it's protected in most constitutional environments so that for a government – if a government wished to do this they would run into constitutional problems.

The establishment of ICANN as a non-government organization surely was not said she, (unintelligible) to avoid constitutional protections on the Internet. Thanks.

Chuck Gomes: Thank you, Stephanie. And to narrow our focus on where we're at now, I'm going to ask you to a question. So can I assume that you're supportive of the possible working group agreement that is on Slide 12 understanding that we may do some tweaks like we did with the certificate issue? Is that correct? Stephanie?

Stephanie Perrin: Can you repeat that please, Chuck?

Chuck Gomes: Yes. Can I – okay I want to bring our focus back to where we're at. You expanded into the other two parts of this purpose. We're just focusing on investigation and we're not talking about access right now, we're just talking about collection. With that understood, based on what I heard you say, you would be supportive of the working group agreement that's shown in orange on – in the orange block on Slide 12 in Adobe understanding that we may tweak that like we did with the certificate purpose. Is that correct? Okay, you can get back to me on that in the chat if you want. Let's go to Andrew.

Andrew Sullivan: Hi. It's Andrew Sullivan here. I just wanted to respond to one narrow thing. So first of all I agree with the orange box on Slide 12. I wanted to respond additionally to one thing that Stephanie said because this isn't only the criminal activity piece, right, there's the DNS part. And it seems pretty clear that the directory service, the registration data directory service that is the result of this is partly there so that you can understand who is the registrant of a given name or at least have some sort of contact with that registrant in order to operate the DNS. And part of the operation of the DNS is in fact to be able to stanch abuses of it.

So I think the DNS abuse part of this puts this – the policies around the use of this data squarely within the remit of ICANN precisely because of the need to support the distributed operation of the DNS. Thank you.

Chuck Gomes: Thanks, Andrew. Rod.

Rod Rasmussen: Thanks. And Rod Rasmussen here. So I agree with what Andrew had to say there. And again, with the emphasis on this is assuming the data is already collected, there's enough value as it has been historically and we'll get into a different place if that's not the case. And I think you know, our sub team is in pretty much violent agreement with what Stephanie just had to say, so I think we're all in agreement on that.

One thing I would point out because this came up in the chat a little bit and with Stephanie's comments is that there are some countries, some legal regimes, where people are required to put their information in – we'll point to China as a great example of that where they've moved to a regime where it's you need to come in person with identification in order to register a domain name. So it can be required. And one of the reasons they're doing it is you know, what many others – people in other countries would be considered illegitimate but, you know, that is their right within their sovereignty to do that.

So there's certainly a place for where governments can insert themselves depending on how they've got their framework set up. But in general for gTLDs we don't have to worry about that, I hope. And as long as enough – as long as data is collected and for other purposes we could talk about this as an access question going down the line. Thanks.

Chuck Gomes: Thank you, Rod. Take a look please at the reformulation that Lisa put into the chat. In case anybody got off of Adobe, I'll read it because it's not very long, just some alternative wording to take advantage of the discussion we had – lengthy discussion we had today on certificates. She rephrased this to, "Criminal activity, DNS abuse" – the investigation part only, okay, "is not a legitimate purpose for requiring collection of registration data but may be a legitimate purpose for allowing some data to be collected or for using some data collected for other purpose."

Anybody have any problem with that reformulation or an objection to polling on that or any suggestions, again, like Alan said, we don't want to edit on the – in the meeting here, it's not very effective. But it would be good if we can test this not only for those of you on the call in a poll but those not on the call. Rod, do you think that the modifications that Lisa made are not needed in this case? And you're welcome to respond verbally if you'd – is that correct?

Rod Rasmussen: Yes, and basically go with what we had before. Yes, no at this point there's no need to – I think we've seen optional need to collect anything for criminal investigation purposes, unless we want to say, hey if you're a criminal please put your home address on this special criminal data field. I could see – I could see there being – I'd love that field. I could see there being a somewhat related kind of thing where you might want to do something as say, a validation around you being a corporate entity X, but that's getting pretty far afield, you know, corporate entity X, as you know, I'm a registered good guy of some sort, blah, blah, blah and that kind of – but it's not really this purpose. I'm putting a very multi-sided peg into a round hole trying to do that.

So I don't know why we would need to say there may be some optional kind of thing we would want to do here.

Chuck Gomes: So, Rod, you would stick with the way it's phrased in orange on Slide 12?

Rod Rasmussen: Yes, and I'm just reading what Lisa asked in the chat, it might – registrant want to provide their data in order to enable an investigation in a protected domain, I guess in the case of a – but this goes into – I could see it in the case of an abuse contact or some sort of reputation service which are two different purposes, and I think that would be the time to maybe add this. And if we're rolling this up into one meta-purpose then it will show up there. I'm just trying – I'm trying to think of a scenario and maybe I'm just, you know, thinking (unintelligible) where you'd have some sort of optional thing which would assist with investigations that you could add optionally as a registrant. I'm not thinking of one but that doesn't mean it doesn't exist.

Chuck Gomes: Okay thanks. Tim.

Rod Rasmussen: Yes, evil bit, yes, evil bit.

Chuck Gomes: Tim O'Brien, you're up.

Tim O'Brien: Hello all. Tim O'Brien for the record. I wanted to expand a little bit on what Andrew was talking about a few minutes ago and also I can understand where Stephanie is coming from but any time we start talking about this it's immediately going to the – I don't want to say fear mongering but getting law enforcement involved. And let's remember and keep in mind that the only time law enforcement gets involved at least here in the US is if the damages are above a certain amount.

There is a tremendous amount of work being done in regards to abusing DNS malware that's being spewed on domains, water cooler attacks, etcetera, that are being handled and addressed both by information security professionals, both in our paid jobs but then also the work that some of us researchers do on weekends and in evenings. The only way we're able to help those companies that are being impacted and affected is by reaching out to them via the information that's currently in Whois.

Now when we go to RDS, we're going to have to get registered to even get access to this information. And logging what purpose, that was the whole intent that came out earlier in these conversations. So when we – we start worrying about these things we need to keep in mind here's the work that's happening on a daily regular basis making sure that DNS is working appropriately, that companies are able to communicate to their customers, to the people trying to access their websites, on a daily regular basis.

Chuck Gomes: Thanks, Tim. And we appreciate having lots of the people in this group now, especially since like spring or so of this year who do a lot of this work, so it's been very helpful to have that – those contributions. Let me jump over to Greg Aaron. Greg, you're on mute. Still not hearing anything, Greg.

Greg Aaron: Chuck? Oh…

((Crosstalk))

Greg Aaron: The moderator is a little slow in joining me, sorry.

Chuck Gomes: That's okay.

Greg Aaron: So one of the things we're trying to do here with this language I think is trying to do a work around. I think the bigger question is various parties need to know under different circumstances who has registered a domain name and then some associated information about the domain name. And that information is used to handle investigations when somebody needs to look at a particular abuse case for example.

It's also used as Rod described, which is to characterize domain names to try to make reputational decisions which is sometimes made on an individual basis by a person and sometimes that's done in an automated fashion by looking at, for example, the name servers or what email address is used to register a domain name, that kind of thing.

What we're saying here is we need to know who registered a domain name and some information associated with it and we're saying that we're not going to collect it for that purpose, we're going to say we'll be able to use it if it's collected for some other purpose. So what are those other purposes? We're relying on the fact that there’s some other reason we’ve collected it. So I’m asking what those are because if we don't nail down what those are then this use case falls apart and it can't be justified.

I’m actually of the opinion that this is a legitimate reason for collecting it along with some others. And I think the collecting and processing of it may actually be allowed, for example, under GDPR. So I think we’re avoiding the real important question here and hope – just hoping to kind of sweep it under the rug in a way. I think it’s actually a legitimate reason to collect. There’s been a separate issue of who gets to see it and under what circumstances. Thanks.

Chuck Gomes: Thanks, Greg. By the way, we will get to the – I’m pretty sure we’ll have to get to purposes for access and we’ve said that over and over again so I think that is something that’s coming down the road so thanks for your input. Now my inclination, but I’m open to suggestions, we have a few – just a few more minutes on this call, is to go with the formulation that’s on Slide 12 for a poll, and of course all of you will have a chance to comment on that, to support it or not support it, suggest edits as you see fit.

Does anybody object to – this would be our second poll item in this week’s poll. And anybody object to that? Any suggestions on that? Okay. All right so – and again we’re not talking about reputation yet, we’re going to get to reputation and notification so keep that in mind as noted on – at the bottom of Slide 12.

So as we wrap – as I wrap up this call, let me compliment everyone on the call for the participation. I think this has been one of the – and everybody that’s in Adobe hasn’t said something but we had a nice variety of people, probably a larger number of different people contributing to the discussion on the call then I recall having. And I like that, that’s really good. So thanks to those of you who don't always jump into the discussion for doing so today. And I hope you will do that going forward and feel comfortable doing that.

That said, let's take a look at our action items and, Lisa, you want to help me out on the action items? I haven't been following the notes very closely. You probably already have them all in there but if you want to just jump in as we wrap this up that would be great.

Lisa Phifer: Thanks, Chuck. This is Lisa Phifer for the record. So I believe the actions are to record the rough consensus on working group agreement on data for domain name management in our working document; to launch a poll to test the new wording for domain name certification as a legitimate purpose; and then to include in that same poll this possible working group agreement on criminal activity, DNS abuse investigation.

Chuck Gomes: Thank you. Any questions on that? The note that our next – our meeting next week, is at the same regular time on Tuesday, okay. That is the – I think the third meeting time of the month but only our second meeting so our alternate time meeting will be on our third meeting, the week – a week later on the 23rd so next week will be at the regular time. Please keep that in mind. Watch for the poll hopefully later today. And again, encourage all of you to participate in the poll. The more data we have the more it helps our follow up discussions and review of the results next week.

So please do that. Two key questions in the poll so everyone's participation, including those not on the call, hopefully they will listen to the recording because there's been a lot of what I think was very constructive input today. So we've come up with a new term, Lisa-fied. Thanks, Rod. And thanks, Rod and Dick for participating. As we move on into the other two areas, notification and reputation, we hope that you'll be able to continue to help the working group on that.

Oh Steve's creation, okay, thanks Rod, for setting that straight. So thanks, everybody. Lisa, you have your hand up, go ahead.

Lisa Phifer: Thanks, Chuck. Steve's term actually was part of the question, which is do you want the poll also on the alternative formulation for criminal activity, DNS abuse investigation?

((Crosstalk))

Chuck Gomes: My inclination is no, that people can comment on that if they think it's relevant, but I'm open to change on that. Okay. All right, yes, Steve, go ahead.

Steve Metalitz: Yes, this is Steve. I would support including that because I think the discussion has convinced me that there are circumstances in which it should be – this would be a legitimate purpose. I posed one in the chat to Rod about a registry dedicated to some type of medical professionals and this would say basically they couldn't collect information about someone's status as a practicing doctor in order to investigate possible abuses that would occur. I mean, maybe that falls somewhere else but it just seems to me there are scenarios in which it should be mandatory to provide this information. Thanks.

Chuck Gomes: Thanks, Steve. I'm good with that. So, Lisa, let's go ahead, maybe we can do it in such a way so that it makes it easier to tabulate the results. Some people might, for example, be comfortable with either one – so you're really good at crafting it in a way that makes it easy to – it doesn't have to be an either or, probably in all cases but we'll work on that. Thanks, Steve, for that feedback, we'll go that direction. Anything else before I adjourn?

Okay, we covered I think quite a lot with all the good input and we're still on time so I will adjourn the meeting now, the recording can stop. Thanks again, everyone. Bye.

Julie: Thanks, everyone. Today's meeting has been adjourned. Operator, (Princess), can you please stop the recordings and disconnect all remaining lines. Have a good day, everyone.

END