ICANN
Transcription
Next-Gen RDS PDP Working group call
Tuesday, 16 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 anauthoritative record. The audio is also available at: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-16jan18-en.mp3

AC recording: https://participate.icann.org/p6iazxg8pt6/

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

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 are now started.

Julie Bisland: Okay great. Thank you. Well good morning, good afternoon and good evening everyone. Welcome to the Next Generation RDS PDP Working Group call on Tuesday, the 16th 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.

Chuck Gomes: Thanks, Julie. And welcome to everyone to today's call. Does anyone have a statement of interest update? Okay, not seeing any hands, I will assume not and let's jump right into the agenda, so if we can pull up the slides for today's meeting, that would be great.

You can see on Slide 2 the agenda. Are there any questions or suggestions regarding the agenda? If not, we will move right on to Slide 3. We're going to review the poll results from our last call and the poll from last week. And we're going to do that fairly briefly because we're not going to declare any conclusions on the results there except that the results kind of motivated us as leaders to change our direction a little bit, maybe backup a little bit like a few people have been suggesting.

You can see in the second bullet there the high-level results of the domain certification question, which was Question 2. And interesting thing is that support for what we thought was a previously forged agreement has fallen from 84% to 67% with a full 33% now arguing that domain certification is a legitimate purpose for collecting some data.

So, there were some good comments. I'll let you review the comments on your own. We're not going to discuss those results today but at some point we'll come back to domain certification after we've done a few other things.

Question 3 was on criminal activity - investigation of criminal activity and DNS abuse. And in that poll, or that poll question, more working group members explicitly stated that investigation is a legitimate purpose for collecting some data than those who did not support that. So it was like 56% to 40% not an overwhelming majority but still strong. And so after consideration of the results from this poll, the leadership team decided it would be helpful to actually spend some time talking about what criteria should we apply to decide what constitutes a legitimate purpose for processing data.

And so that's what we're going to focus our time on today. If anybody has any questions on that or the change of direction again, we'll come back to those two purposes later, but if anybody has any questions or comments on that, that would be fine, otherwise we'll jump right in and go to Slide 4.
Again, everyone should have control of Adobe so you're able to jump around as you need to. On Slide 4, again, we repeat the - what makes - some of the

criteria that we've put on slides for quite a few weeks now. The first one was, "Does it support ICANN's mission?" And Slide 12 and after that in this particular deck, although we're not going to go through those today, but you're welcome to look at those are the - some key statements in the bylaws about ICANN's mission.

And some of you - I'm thinking of Greg Monier in particular, provided some good feedback in terms of what the bylaws say with regard to security and so forth. So hopefully all of you saw that.

Next criterion was, "Is it specific?" The third one is, "Is it explained in a way that registrants can understand?" Fourth one is, "Does it explain to registrants what their data will be used for?" And, "Is it necessary for the fulfilment of a contract?"

Now, all of those are clearly related to the GDPR and other regions that have similar regulations. And those are important things when we're dealing with policy implemented for those regions where they apply. But we're going to - and we need to assume that we'll have to deal with those when we get to that point. But, in terms of deciding whether particular data elements should be collected and ultimately accessed, I think it'd be helpful if we have some other criteria and focus on those before we come back in implementation and talk about whether the - anything we recommend is specific enough or whether it can be understood by registrants, etcetera.

So we have some examples of some possible purposes or criteria for purposes that staff has excerpted. So if we could bring up the document that has those? Now this is just taken from two sources. Everyone's welcome to make suggestions from other sources or even your own thoughts in this regard. But we thought it'd be helpful if we looked at some of these things to get the discussion going as we try to develop some further criteria for - criteria for legitimacy, okay, of certain purposes.

Now, the example - these are just examples to help us get the discussion going. You can support them; you don't have to support them. But the first set of examples comes from the GDPR itself. And I think they're really relevant to the discussions we've been having. I highlighted in yellow - now these are excerpts from the GDPR, okay, so you can see the context. But I highlighted in yellow certain things that are mentioned in the GDPR as possible purposes.

You can see there humanitarian purposes, monitoring epidemics, humanitarian emergencies, natural and manmade disasters, going down to some specific examples below they mention scientific or historical research purposes or statistical purposes which gets to a purpose we haven't yet gotten to in this series of our deliberation.

Going down a little bit further, preventing fraud, they even say “direct marketing” okay. They say “network and information security” which some of you have been pointing out as a legitimate purpose. They - and if we look at the first memo from Hamilton, they pointed out in talking about the GDPR, you know, preventing fraud, invoicing, support and other administrative actions, which we’ve kind of covered in our domain name management purpose.

Investigate fraud, which is one of the things we were looking at in the last couple weeks, consumer deception, investigating consumer deception, intellectual property violations and other violations of law. Verify the identity of a provider of goods or services on the Internet, including for consumer protection, identify the owner of a domain name for business purposes. So these are all just some examples that are from really documents related to the GDPR, the GDPR itself in the first case and Hamilton’s analysis of the GDPR in the second case.

So you can see that there are a lot of examples that relate to what we're talking about with regard to abuse and probably even with regard to certificate authorities and certificate actions. So let me stop there and open it up for discussion. Jim, go ahead.

Jim Galvin: Thanks, Chuck. Jim Galvin for the record. Just something to clarify, Chuck, and I want to be a little careful here because I think this kind of stuff is important. There really is a difference between purpose for processing and purpose for collection. It seems to me, and correct me if I'm wrong, please, aren't we focused on the purpose of collecting data because a lot of - all of these things which are now in this document which is from GDPR, up here at the top so the thing which is currently displayed, are really legitimate purposes for processing data, not for collecting it.

So it's something that you're allowed to do with the data once that you have it. You get into discussions about the interest of the data in the second half down below and that's a little more subjective, that's not a given. So I want to make that important distinction, all these things at the top that you were talking about, you know, humanitarian, statistical purposes, preventing fraud, marketing, they're all processing purposes, not collection purposes. Thank you.

Chuck Gomes: Jim, a question for you. This is Chuck. Isn't collection a subset of processing?

Jim Galvin: Not the way - well, maybe lawyers might have a better idea about all of that. But, no, not in my opinion. The way I have been approaching this problem space, and as I understand it, and I am just a layman, you know, you need to - this is where you need to establish your legitimate interest and that's what allows you to collect it and then once you've got it you get to talk about what you can do with it which is within bounds that does not require consent, for example, that's the way I lay out the sequence of events.

So it's legitimate interest, collection and then processing and that's the way I lay out the problem spaced in my mind when I think about it. Thank you.

Chuck Gomes: Thank you, Jim. And I confess I'm a layman like you, okay, just happen to be in the role of chair so I'm just trying to facilitate progress. And I looked at it pretty much the way you did, but our polls have shown pretty clearly that there are a lot of people that are having problems separating the collection from access and processing and so forth. And so that's why we're having this discussion today to see if we can't move forward and reach some understanding of what makes a purpose for collection legitimate. And we obviously have people on both sides of the issue in this working group. Does anybody else want to comment?

Notice that Bradley's comment in the chat, I'll let you read it, and we will get to data minimization, that's going to be important thing. So Marc, go ahead.

Marc Anderson: Hey, Chuck. Marc Anderson for the record. First I want to say I think it's a, you know, I applaud the leadership team's decision to sort of take a moment to step back and look at criteria for what is a legitimate purpose. I think this is a good move and, you know, I'm hopeful this will help the working group in moving forward.

But I raised my hand sort of in response to what Jim said that collection is different from processing, because I'm concerned that like you I was working under the understanding that collection was considered a type of processing. So now I'm concerned that I've been operating under a misunderstanding here. So I was - I'm hoping we can get somebody with a better understanding of processing and collection to maybe set the record straight for the working group, and, you know, is or - is collection a type of processing or not? And if they are separate, I would love a better explanation of why they're two separate things under GDPR. Thank you.

Chuck Gomes: Thanks, Marc. Anyone else want to jump into this? Okay, let's go back to our main slides please. Notice Steve's - Steve Metalitz's comments in the chat that GDPR defines processing to include both collection and disclosure, okay.

And Maxim has a comment in that regard as well. I'll let you look at the chat there.

Let's go down, hold on a second, I need to go down to Slide Number 5, what makes purposes - we've agreed on two purposes already for collecting data, okay? That's a Working Group Agreement 46 and Working Group 48 that are shown on Slide 5. And we had pretty strong rough consensus on these two agreements.

What makes the purpose of technical issue resolution and the purpose of domain name management legitimate? Could we brainstorm a little bit and people share either in the chat or verbally what makes, you know, we had pretty strong support for both of these. What makes them legitimate?

Go ahead, Jim. And we'll capture these in the notes. Okay?

Jim Galvin: Thanks, Chuck. Yes, so thanks, Chuck. James Galvin for the record. I'll just sort of take a stab at this. I'll use a word that I used a long time ago in the early parts of this working group when we first started. For me when I think about you know, these two things on Slide 5 about management and technical issue resolution, for me they fall into the category of self-evident. And what I mean by that is it doesn't make any sense to have this domain name industry if I somehow can't keep track of the industry. I'm trying very carefully to use words that are not circular, right.

So I need to know that, you know, a name exists. I need to know things like who has it because I'll want to continue to sell it to them. I mean, if there's going to be an exchange of value here, the parties need to identify each other in some way and know who they are. And notice I'm not saying "identity" I'm just saying I've got to be able to identify each other to exchange value. So, you know, I need to be able to manage the system. To me that seems self-evident.

The technical issue resolution is closely related to self-evident, although I will concede that it's not exactly the same thing. But, you know, if the goal here is to have an industry in which I'm exchanging value between two parties for whatever that is, you know, sometimes things will happen as a result of being able to do that. And so I'll want a way to make sure that I can maintain contact with those few people or I want a mechanism for dealing with those kinds of issues.

So for me the thing that makes those two purposes on Slide 5 what makes them valid for collection is that they seem self-evident to me. It doesn't make any sense to do what we're doing without those two things. Everything else doesn't feel the same way to me or at least it's not quite as high up on that bar in my mind. Thank you.

Chuck Gomes: Thanks, Jim. Let's go to Mike and I'll - may come back to you, okay? Go ahead, Michael.

Michael Hammer: Hello, everybody. So I find it interesting that James is positing this in terms of the domain name management industry. And he's talking about exchange of value and whatnot. And if we look at the early days there was no exchange of value, you simply said, I want a domain and you got a domain. So I would suggest that for these two working group agreements, rather than talking about exchange of value and industry and things like that, because you can have free domain names, it's inherent to the functionality so if you can't manage domain names then DNS doesn't work.

And if you can't resolve the technical issues associated with domain name resolution, then it simply doesn't work for some scope of not working. And I'd like to bring this back to the broader issue of why we seem to have the disagreements that we have. And I perceive it as more of a scoping and perspective issue, that is there are folks who are very, very focused on GDPR and privacy requirements and regulatory requirements; there are folks who are very, very focused on anti-abuse and combatting fraud; and I'm seeing

Stephanie's comment. But permitting further commercialization does not mean that commercialization is the sole reason for the Internet. There's lots of noncommercial uses.

But anyways, really we can define our discussion solely in the context of GDPR or we can incorporate GDPR considerations into the wider scoping of how does the Internet function. And I've heard several of the privacy experts say - well, they're not really experts on some of the underlying technical issues. But this is really where I think the conflict is coming from because it's kind of like the blind people and the elephant, right, depending on what part of the elephant you're touching it impacts your description of the elephant. And I think this is exactly what we're struggling with here. Thanks.

Chuck Gomes: Thanks, Michael. Appreciate it. Now I'm going to try and - unless somebody else wants to do it and I welcome that - see if we can formulate - and I'll throw something out a reason - a criterion that applies to the two agreements we have in front of us. Okay? Would it be accurate to say that one criterion that's for a purpose for collecting data or processing it, whichever term we want to use, is to ensure that the domain name system works as it's supposed to. Is that a way to phrase what you said, Jim, and what you're saying, Michael?

And I welcome rephrasing of it. I'm just trying to get it going here. Jim, go ahead.

Jim Galvin: You know, I was going to say something but I think I'm going to withdraw so let me just agree with you for the moment. And now that see Andrew's hand up…

((Crosstalk))

Chuck Gomes: Okay.

Jim Galvin: …I'm more interested in hearing what he's going to say about it. Thanks.

Chuck Gomes: Okay. Well feel free to disagree later, that's okay. I'm just trying to get it started, okay? Andrew, go ahead.

Andrew Sullivan: Hi, this is Andrew Sullivan. So every time I hear anybody within, I don't know, 300 miles of an ICANN meeting saying anything like "make the Internet work," I get really itchy. The - ICANN's role is really tightly bound by its mission. And we spent a lot of time on this a couple years ago precisely because there is this tendency for people to make these big claims.

But there is a very narrow problem here and it is to, in respect of certain parts of the domain name system, just certain parts of it. And that part is the infrastructure part that happens to have a public comment. So we have these domain names like Com and Organization and Info and Biz and prospective Web and so on that are places where people can create other domain names, that is they can get new delegations from the domain names.

In the Web world these are called the public suffixes and in the DNS world they're called delegation-centric domains. That is you create names - you create other names in there, there's no purpose to the name itself except to contain other things, maybe there are some corner cases but that's really the main point of it.

When you have a distributed network like the Internet, and when you have a distributed naming system like the DNS, it is handy to have a central place where you coordinate those things and that's what we got ICANN for. And so the reason this is a legitimate thing is because we've got a distributed network with no necessary prior contractual relationship among the participants in the network who need to be able to coordinate their activities with one another with a minimum of centralization, that's the whole design of the Internet.

This ICANN policy thing is the minimum centralization that we need and therefore we create a system by which the individual actors within this larger network can coordinate with one another directly rather than having to go through a contractual relationship all the way up to the center the way you used to have to in the phone system. What makes therefore these two purposes legitimate is precisely supporting the nature of the Internet and its distributed operation.

We've been over this several times so I'm kind of surprised that we have to keep revisiting this. This was the central point. And so the reason that the data collection is legitimate in at least those cases, is precisely because you can't have this system without having that kind of data collection; it's just not possible.

And I think that that minimum criterion for the necessity of collecting the data in order to make the thing work is as far as I can tell what this data minimization criterion amounts to. So I have to agree with Michael's earlier point which I notice he remarks again in the chat, this is inherent to the functionality; you can't have this system without it. And I think that that needs to be the function, you know, the tech that we're trying to meet for the data collection.

I don't know whether there's a difference between collection or other kinds of processing, and I don't care. The real question is once you've got this data, does it support these necessary conditions? And then I don't know, given the nature of the system, I don't know how we can care about the further processing of it after that because of the nature of that distributed system. What do you need to have access to it when somebody needs to have access to it for some purpose, there's no way literally to make a distinction between what their real purpose is or not except, you know, for people to set the evil bit on their intention, and we know that that doesn't work. Thank you.

Chuck Gomes: Thanks, Andrew. And let me point out that I intentionally did not use the word "Internet" I did use the term "DNS" and you clarified that it's some parts of the DNS, and that's fine. I think you said some things that might actually work for a criterion that particularly applies to these two agreements here. Hopefully we can go back and capture those and we'll probably do that. So, Andrew, if you could kind of formulate - you had a couple sentences there, maybe either one of them would have probably worked, if you can kind of phrase those in the chat in terms of why these purposes are legitimate, that would be great. So let's go to Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. I would just note, before I launch into what I'm going to say, that sometimes Andrew and I appear to agree and then the next minute we're having violent disagreements. So I say this with some trepidation because I think we agree but he may think we're violently in disagreement once he hears what I have to say.

The point about the need for ICANN's portion of the Internet to function, the portion of the DNS to function without contractual agreements between parties is equally true for the protection of personal information. And it's one reason why data minimization and proportionality are so central to the collection and use and disclosure of personal information. We have solved this problem of not having contractual arrangements since the inception of ICANN by making it all public. And surely by now we have realized, after 18 years, that this doesn't accord with data protection law and we need other arrangements.

The reason why the absence of contractual arrangements between parties is so important here in the context of data protection law is that it's in the law; if you disclose personal data that you have collected of your customers, that you gathered from them for a specific purpose, namely registering a domain name, and willy-nilly disclose it, you are not following data protection law. Every data protection law has causes in it that say you will ascertain whether the data is being protected to a similar level and if they don't have law and there are no treaty arrangements and there are no adequacy determinations, then you have to protect it by contractual clauses.

So getting back to the importance of data minimization, given this framework for data, you really have to minimize the collection.

Chuck Gomes: So this is Chuck. Those are all good points, but I want us to focus on the question that’s at the bottom of Slide 5, what makes these two purposes, in 46 and 48, legitimate for processing registration data? Could we focus on that, please? Marc, go ahead.

Marc Anderson: Thanks, Chuck. It’s Marc Anderson. I want to follow up on what Andrew said. You know, I thought he made some really good points and I agree with what he said. But I raised my hand when he pointed out that he's made the same points multiple times and he has, this - it’s not the first time he's done that. But I think what Andrew was doing was laying out purposes for RDS. And we’ve been focused largely you know, in recent weeks on purposes for collection of RDS data.

And what Andrew did was, you know, I think he did a very good job of, you know, of explaining a purpose for RDS. And I think that’s really important and I think we should take sort of what Andrew said to heart that, you know, you know, he keeps having to make this point. And I think it would be worthwhile to try and take what Andrew said and consider it for a possible working group deliberation for consensus as a purpose for RDS because I think if we had, you know, Andrew’s purpose for RDS in mind it would give us one of your, you know, what we’re doing today is looking for objective rather than subjective criteria for purposes of collection for the data.

So I think if we had Andrew’s point you know, succinctly summed up as a purpose that we could, you know, deliberate and hopefully agree on, I think it would help us moving forward, you know, in looking at these various purposes for collecting data. So, you know, Andrew, you know, I think you did a good job, hopefully you'd be willing to sum that up in sort of words that we could consider for working group consensus. Thank you.

Chuck Gomes: Thanks, Marc. Is that an old hand, Stephanie? I assume so. Let me go back here to the chat. I'm focusing on what Andrew wrote in the chat so I think that the DNS is the Internet's primary naming system and it needs a registration directory service to make the Internet's decentralized operation work, and particular to make a system that does not require preexisting contracts among everyone; everyone involved in the operation needs to be able to contact one another. That's why 46 and 48 are legitimate purposes for collection.

Let's talk about that. Does that work? Is that - and I think the first part of that is what Marc was referring to as a justification for the need for an RDS and the second part I think, Andrew, seems to get right into the question what makes these purposes legitimate for collecting data. What do you think about the way Andrew formulated that in the chat? Does that work for a - we can refine it later, but if it needs to be, I don't know if it needs to be or not. Is that what makes these purposes legitimate? Does that express it well enough? Greg Shatan.

Greg Shatan: Thanks. It's Greg Shatan for the record. And I just - to echo what I said in the chat, Andrew's approach and analysis make a lot of sense to me and echoes something I tried to say last night in the email list which is that we, you know, really need to understand, you know, the value and importance of RDS to the ecosystem or structure or whatever we want to call it. And that's I think where Andrew is getting at or that's in one of the kind of the tent poles of Andrew's analysis. And, you know, kind of trying to pretend that RDS isn't really something that's necessary and valuable and without which things would fall apart to say the least, I think you know, that's where a lot of the trouble comes from trying to carve things so thinly that we tend to forget the interrelationship between the different aspects of what we're doing.

So again, echo what someone else said and praise the idea that you and the rest of the folks helping us move along have taken this step back. Thanks.

Chuck Gomes: Thanks, Greg. So if we could put the - take Andrew's statement there just as it is without any changes that starts out I think that the DNS is the Internet's primary naming system, if we could put that over in the notes area so people don't have to keep scrolling up to it that would be helpful under a list of possible criteria for legitimacy, that would be helpful. And then we'll leave that there and does anybody want to add to that or qualify it or comment on it further before we go to the next slide?

Okay. Then let's go to Slide 6. The - what other - and again we're not going to focus on 1-5 up there but rather we're going to look at other criteria so what I'd like you to think about now and just kind of open it up, so we have a possible criterion statement for domain name management and technical issue resolution.

What are - not restricting yourself to those two, in fact for any purposes, what are other criteria that we can use to measure whether or not collection of some data is legitimate? What are some other reasons - I know a lot of you think there are lots of other reasons for collecting data. What would make them legitimate? What are - let's see if we can't formulate some ideas and then we'll try and narrow them down or refine them as necessary.

A lot of you - 33% of the people who responded to the poll said that domain name certification is a legitimate purpose for collecting data. What makes it legitimate? A majority of those responding to the poll felt that domain name abuse investigation is a legitimate reason for collecting data. What makes it - what makes those legitimate for those of you who responded to the poll in that way?

I'm pretty sure that silence doesn't mean that you don't think they're not legitimate. What makes them legitimate? Marc, go ahead.

Marc Anderson: Hey, Chuck. It’s Marc again. I guess I have a question to your question, which I feel like is kind of bad form, but I’m going to do it anyway. When you asked on the - your example, you know, what makes the collection of data for certification purposes legitimate? Are you asking - I think the question varies. Are we talking about requiring data to be collected for the purpose of getting a certificate or is it a legitimate reason to collect the data at all?

So I think you know, from my perspective, you know, if, you know, if I’m a domain name registrant and you say I must provide certain data because I might want to get a certificate for my domain name, that doesn't really sit right with me. But if I hear that, you know, collection of data for purposes of getting a certificate is legitimate, and it’s up to me as the registrant whether I want to provide for that purpose, you know, I think that, you know, that makes sense.

So you know, if you're saying it’s a legitimate purpose for requiring the data I’m not sure I agree with that, but is it a legitimate purpose? Sure. Does that make sense?

Chuck Gomes: It does. In fact we’ve spent a lot of time talking about that last week on the call. And in fact, we reformulated the certificate - the proposed certificate agreement to distinguish between required or just legitimate for collecting more on an optional basis. And then we - the statement we formed for domain name abuse investigation was similarly formatted to make that distinction.

So for the sake of this discussion, let me suggest, unless there’s objections to this, that we go with the latter formulation. Let’s worry about whether we would require collection later and just come up with some things that would make providing such information legitimate, whether it’s required or not. Jim, go ahead.

Jim Galvin: Thanks, Chuck. James Galvin for the record. So I guess I want to say a couple of things here. So let's kick off the discussion by saying something both rhetorical and proactive, this ought to help people along in this space, okay. I think that technical abuse analysis is not a reason for collection of data. Full stop. It is not a purpose at all. So here's an analogy that one could think about, and we all know how imperfect analogies are so I don't want a discussion of why my analogy is imperfect.

But I think it helps make my point about why it's not at all a reason for collection. You know, to suggest that I have to know who you are because you might, you know, do something abusive with your domain name, or something like that, is sort of akin to the idea that I should fingerprint and DNA collect every citizen because they might break the law and I need an easy way to identify them. Okay, so I mean, that's sort of an extreme kind of point of view but it carries forward this idea that abuse is not a reason for collecting any data.

But one of the things - the second thing I want to say then - so that's just sort of one point to be provocative and rhetorical. But on the other hand, my second point is that I very much support technical abuse analysis and I completely support the idea that there are operational considerations and there is great value in having some of this information and having it available. So I make the following observation in my mind, one of the things I've never heard us talk about is the fact that as far as I can tell there is no data that we're asking for in that category, all right, that is not already being collected and mandated for other reasons.

If we already agree that you have to collect the who information and identity information about an owner or at least you have to collect contact information, about a responsible party, as opposed to necessarily the identity of the owner of a name, then I think the only issue we're really talking about is whether or not you should have access to data that's already there. I guess I struggle in this conversation to understand why we're focused on is technical abuse a reason for collecting data when as far as I can tell the data they want is already mandated for collection.

So why can't we delay this conversation for discussions about publication? You know, I hope I'm making my point here. And I can try to summarize in two sentences my two points if you need it but I'll just pause. Thank you.

Chuck Gomes: So, Jim, what do you mean "mandated for collection"? What data is mandated for collection?

Jim Galvin: So our - the thing there which is in our - on Slide 5, you go back to Slide 5 we say "Domain name," you know, "management," okay, I mean, you need to be able to collect an authorized party, all right, so you need to know who an authorized party is about the name. And I think that that is - we're sort of going down the path I believe, I mean, this is for you to judge but I'm sort of assessing my assessment of the group here. We're agreeing that that's sort of mandatory for collection, that kind of data, that that's a legitimate purpose for collection of data and that essentially mandates the collection of that data.

What I'm wondering is, is there anything else under technical abuse that we're trying to get access to? Is there something else we want that's not already there? Why are we struggling to agree on collection of something for abuse when there's nothing new to collect? At least I don't think there is. Thank you.

Chuck Gomes: Okay, thanks, Jim. And so when you said "mandated" we've already agreed that this data should be collected for technical issue resolution and domain name management. And so the - and by the way, I think that Andrew in the email discussions the last couple days made the same point you're making that say we've agreed that data should be collected here, let's move on from there. And maybe that's what we should do.

So I guess the question - and I think you kind of asked this, Jim, are there any other data elements besides those we've identified for technical issue resolution and domain name management that need to be collected for any other purposes. Did I phrase that right, Jim?

Jim Galvin: Yes, thank you.

Chuck Gomes: Okay. And I'd like people to respond to that after I go to Rod. And, Rod, you're welcome to respond to that too.

Rod Rasmussen: Thanks, Chuck. This is Rod Rasmussen. And I am kind of - yes, I'm responding to that. I want to agree a lot with what Jim just said there. I mean, Jim and I don't always agree on these topic and scope issues. I'll throw another imperfect analogy out there that I think is slightly better imperfect analogy, that's, you know, automobile registration, rather than, you know, fingerprinting everybody, but the idea being that I need that for an - in order to change ownership and all that other stuff, but I also need it to track down, you know, whose car may have been used to commit a crime or if it was stolen or something like that.

So but again, analogy, imperfect, blah, blah, blah, all that - all those disclaimers. But I think that's a good way of thinking about this from the point of view that Jim was just speaking to which is I've got to collect all this information anyways and I'm sure most of you know that I would love to make this a primary purpose of collecting data as to prevent fraud and abuse and all that.

But I think we may spend a whole lot of time arguing about that as a collection criteria when if it's already being collected for just making the dang thing work and the system work, etcetera, and it's already there it's, you know, we can get a hold of it. I think the answer to your question, Chuck, is well why would we, you know, why are - is there - and to Jim's question, is there any other data that we would want to have that would be legitimate. I could come up with all kinds of data that might be required in fact, you know, if you take a look at Chinese domain registrations, they require a - you to - and at least I'm not sure if they still do but they were for a while, they were requiring a physical ID and they'd take a copy of it. Right?

So and ostensibly that was one of the reasons for that was because of all the rampant crime that was going on over dotCM. So you could require more data. I don't know that anybody is going to agree to collect more data for the purpose of investigating, preventing, etcetera, crime, fraud, abuse, etcetera. The access to the data we are already collecting for the management, use, name, ownership, transfers, all these things that we've been talking about from a - just using the darn things and making the Internet work, is sufficiently adequate for our purposes from a - from my perspective maintaining access to that data in some form or functionality is of utmost importance. I don't care about the why it's in the system, I care about that I can get that information in order to be able to do the things I need to do to prevent the Internet from becoming more of a cesspool than it already is.

So if we can skip past arguing about whether we need to make this a collection criteria as long as we know it's going to be there for some other reason then that's great and we can continue to make progress. It's just this gets to an access slash processing issue. Thanks.

Chuck Gomes: Thanks, Rod. Steve Metalitz, you're next.

Steve Metalitz: Yes thanks. This is Steve. I think there might be at least two reasons why people are concerned with the approach that Jim just put out and that Rod supported. The first one is an issue that comes up on the list periodically, it came up again last day or two, and that is this whole issue of information or data collected for one purpose being used for another purpose or I should say being processed by means of dissemination for another purpose if it's - if the purpose for collecting it is different.

It may be helpful - I know that's a European you know, kind of a Euro-centric concept but it also appears in other privacy laws and in fact it appears in the OCD guidelines which are among the most comprehensive statement of data protection principles. So it might be worth having - and I think Nathalie suggested this on the list - maybe it's worth having that greater clarity about whether if we agree - we were all to agree that for example combatting - investigating DNS abuse is not a legitimate purpose for requiring collection of data, what impact will that have on the ability to use the data that's collected for another purpose, use it for the purpose of combatting DNS abuse. So that might be one issue where we could get some greater clarity on that question. And it might put people's minds at ease.

The second one which I think also applies, although I don't have a concrete example to give you, is that, you know, the data that's necessary for a particular purpose might change over time. And it's certainly possible that data which is today considered necessary for, you know, for the technical issue resolution, domain name management purposes, might in the future become unnecessary for that purpose and therefore I suppose under data minimization it should no longer be collected for that purpose.

Well if that data remains essential for another purpose, such as combatting DNS abuse or criminal activity or obviously there's a lot of others that are among the legitimate purposes that have even identified in the GDPR and in that commentary that you showed, so if it's no longer necessary for the technical issue resolution or domain name management purpose, then do we have to go back and say, oh yes, but by the way, we do think it's necessary for this other purpose and we'll now decide that is a legitimate purpose even though we decided initially that it wasn't a legitimate purpose.

So I think those might be two reasons why - speaking for myself, those are two reasons why I'm uneasy about agreeing with Jim and Rod's proposition that we just shouldn't worry about it because if it's being collected for a unassailably and universally recognized legitimate purpose like technical issue resolution, well we can always use it for these other purposes as well. Thanks.

Chuck Gomes: Thanks, Steve. This is Chuck again. And before I go to Michael, I am absolutely not a GDPR expert. And there are many of you on this call that are much more expert about it than I am. But my understanding is just because something is collected for one purpose, doesn’t give you the right to use it for other purposes.

And I think Steve’s right, and I think this is your first point, Steve, is that it may not be sufficient at least in cases where the GDPR is involved, in other words, the European jurisdiction or other jurisdictions that have similar regulations that it actually - if we don't identify for example the registrant name be collected for abuse investigation, and we just decide to provide access to that because it’s collected for another purpose, I don't think that works, does it, under the GDPR? Or are there ways to get around that?

Again, I’m looking for those of you who are more expert in that but I think that both of Steve’s points are valid but that’s the one that really jumps out at me. I would be really happy if we could just say okay, we’re collecting these data elements for the purpose of technical issue resolution and domain name management so it’s okay to use them for another purpose whether it be certificates or abuse investigation. I don't think that works but that’s my - based on my limited reading and understanding of the GDPR. So let me go to Michael. Go ahead, Michael.

Michael Hammer: Thank you. Michael Hammer for the record. I think what we come back to is ICANN’s mandate regarding stable operation. And I think this is really important and so I’m going to say the whole thing again. The mission of ICANN is to coordinate the stable operation of the Internet’s unique identifier systems. And we know that the abuse going on negatively impacts - significantly negatively impacts the stable operation. And so I think that in itself is justification.

The other issue - the other reason for including it as a legitimate purpose from ICANN's perspective and it being anti abuse, is that without ICANN specifying this, then it becomes the decision of each registrar, each registry, as to whether or not it's legitimate, who gets access, whatever, and the only way that this is going to happen on a consistent basis is through the contractual relationship between ICANN and the registries passing down to the registrars.

And so that is a very compelling reason for ICANN to determine whether or not it's a legitimate purpose. I believe that it is but I think this is something where I will state it in a more neutral fashion because really it's a decision. Do we want a consistent playing field or do we want it to vary significantly.

And quite honestly as an operations type person, to those who consistently say we don't need this as a legitimate purpose, blah, blah, blah, careful what you ask for because as I've said in the past, the folks who actually operate where the rubber meets the road, will have no problem blocking those folks that they view as being involved in abusive activity. And if it has to happen at scale for particular registrars or even registries, it will happen. That's all I have to say on that.

Chuck Gomes: Thanks, Michael. Chuck again. Everybody might want to look at Slide 12 and I think what Michael was - shared at the beginning there was really Paragraph A under the mission there as part of the bylaws, and then he talked about some other things. You might also look at the red highlighted bullet that's part of that mission that talks about to facilitate openness, interoperability, resilient, security and/or stability of the DNS. I think this is probably one of the things that Greg Monier included in his references and his posts the last few days. So I just wanted to call everybody's attention to that.

And of course one of the things with regard to registry and registrar agreements, if we as a working group recommend some policies ultimately and they get approved by the Board, they will become part of registry and registrar agreements. And I think everyone knows that, that's the ultimate goal of where we're trying to head in this working group, although it's a ways off right now.

Let me go to Jim Galvin. Go ahead, Jim.

Jim Galvin: Thanks, Chuck. James Galvin for the record. Just want to thank Steve Metalitz for his you know, comment about the reason why we want to care about other potential purposes for collecting the data. You know, I appreciate that. Let me make the following observation about that and I think Rod was sort of saying some of this in the chat room here a moment ago, I'm going to use my words because I think I agree with what he said.

And let me offer it up in the following way. I absolutely agree that we do have to do, you know, give due consideration, due diligence to be thinking about the future. It is always possible that the world is going to change and circumstances are going to change. And we should give some consideration to the likelihood and probability of that and our concerns about it and try to account for and accommodate as much as we can.

So even though I agree with that, though, and Phil, I appreciate your comment in that context, I want to come back to the other half of the question that I asked which is just that is there other data that we need to consider that's not already being collected because I think that the forward thinking question that you're concerned about also has a backward thinking question we have to care about and that is if you're already getting the data that you want and then as Rod said in the chat room, you know, there is a whole industry you know, and in fact I think ourselves as an industry that care a great deal about the processing that is necessary for technical abuse, I really see the likelihood of this stuff going away you know, quite limited.

And so the data has got to be collected and the data being collected is not going to change. And I also think that you're going to get very strong support from a broad base of the community that we also need to be able to do technical abuse on this data. One of the things I think this working group needs to do is you mandate for collection, you know, for inherent to functionality purposes or what I, you know, like to call self-evident but maybe inherent functionality is the preferred phrase, but we can also say that as part of ICANN's mandate and mission to support correct operation, you know, here is a processing purpose that has to be essential.

So now that you have this data this particular purpose is also essential to the operation. I'm, you know, negotiable on whether that means it has to be a mandated collection reason but it, you know, it certainly is something we could recommend and mandate I think at a minimum as a processing reason. And it gets us forward, it gets us forward. And I don't think the future puts that at risk quite honestly, although I agree we should ask ourselves the question, I really think that's a pretty low risk because I also think it's a pretty low risk in the future that we would ever decide to collect less information that we already are because there are just far too many of us for far too many reasons that we'd ever see that go away. Thank you.

Chuck Gomes: Thanks, Jim. Let's go to Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. Marika has placed into the chat a very important chunk on the GDPR. I'm going to also urge everybody to read all the preamble because a lot of the processing - further processing of data - and I'm speaking to the point that Steve Metalitz has raised, the requirement to process only for the purposes collected. There are always exceptions to that in a free and democratic society where the rule of law pertains, you can release data under appropriate authority without listing that as a purpose for collection.

And we have been told in the data protection commissioners' letters, notably the one from the head of the Article 29 group during the RAA negotiations in 2012, that would be (Yacas Cunstam), that retaining data solely for the purposes of law enforcement potential use was unacceptable. Now, we got the same thing from the EDPS in 2014, that would be the (Hasting)s letter. So data is available as Rod and Jim have said. We're not going to stop collecting this data that is necessary for technical requirements, and it can be made available under a tiered access system rather easily for all of these purposes.

So I wish we could stop this discussion of things going dry. Yes, it's going to be more difficult, but it's high time it became more difficult. Thanks.

Chuck Gomes: Stephanie, this is Chuck. I'm going to come back to you because you obviously studied all this very closely and it's been your life for a long time. I'm going to come back to the issue that Steve raised, his first point, and then my follow up. So - and you've been one that has advocated, hey, like you just said, the data is there, what we need to deal with is access. Is it sufficient under the GDPR and similar regulations to define a purpose for access that's different from a purpose for collection? Would that be allowed under? So for example, to be very specific, we have defined agreed mostly, okay, and rough consensus - strong rough consensus - that certain data should be collected for technical issue resolution and domain name management.

So we have some data elements there that are already being collected. Under the GDPR and similar regulations, can we then use that data for other purposes which the data was not collected for? That's what's not clear to me. Did my question make any sense? Stephanie, this is to you.

Stephanie Perrin: Yes. Yes, it's Stephanie again, for the record. And I'm heaving a great sigh because I've been at this for such a long time having been a data protection officer in governments in 1984, believe me, debate with law enforcement about whether they need explicit recognition to get data spelled out when in fact they have the power under the law is tiresome. We have put it in - we put it into the data protection law in Canada even though not necessary because they didn't want to bicker about it for political and public relations purposes.

That does not seem to have been the case in the European law possibly and I don't claim to be an expert on GDPR, although I have certainly some familiarity with it. I think that it’s worthwhile asking whether pulling out under the disclosure stuff that we haven't got to specific instruction about disclosing, you know, subject to applicable authority, blah, blah, blah, is - would help and would help get us past this roadblock. I know we caved into it when I was drafting the Canadian law just because we weren't going to get it through Parliament unless we did, but it was unnecessary. I would point that out again.

Now obviously ICANN’s dealing as has been pointed out in many legal jurisdictions, so I think the arguments for making it explicit is much stronger, but I keep saying if you put it into the purpose for collection you will immediately find yourself in court because that’s like waving a red flag in front of a bull to civil society. We do not, as ICANN, collect personal information for the purpose of facilitating law enforcement and anti-abuse and consumer protection. Consumer protection in particularly - in particular is far too loose because it gets us into content rather quickly. And that’s a slippery slope.

So I think we should investigate that when we look at our disclosure policies. It’s - the passage that Marika cited will get us there and you may recall that (Tanatachi) in Copenhagen was perfectly willing to discuss this further, I think we should follow up with these guys. Thanks.

Chuck Gomes: So a question I want to raise before I go to John is should we - looking at Marika's statement, be focusing on processing I think that’s at a higher level, instead of focusing on collection. Would it help if we talked about purposes for processing or do we need to be even more specific and move ahead and start talking about access? I’ll leave that for now and go to John.

John Bambenek: Can you hear me?

Chuck Gomes: Yes. A little low but yes.

John Bambenek: Hello?

Chuck Gomes: Yes.

John Bambenek: Okay. Is this better?

Chuck Gomes: Yes, it’s a little better, yes. Thanks, John.

John Bambenek: You know, just listening to - yes, listening to what Stephanie says, right, it goes back to a point you need to make, right, that I can put my phone number on Twitter if I want, I can put my email address on Facebook, I can post pictures of Instagram in various states of undress of myself because I have free consent. Right, or I can consent freely to do so, right, by making it public.

We keep going down this road because we assume the status quo that we will not - that registries will not provide the option without a charge for people to not publish their data in the RDS. All of this discussion goes away almost immediately simply with one thing is that if I can register a domain and free consent what information is published about me so that people can contact me, that I am aware of the pros and cons of doing both almost everybody is satisfied immediately.

But we don't talk about that issue except when I raise it because Twitter has solved this. If I’ve got a public Twitter account and I publish whatever I want on there, I can publish my social security number on there, that is not on Twitter, that is on me. If we make it an option for people to put data into RDS, or whatever the successor system is, and just say this means anybody in the world can contact you here for reasons of abuse, for reasons of law enforcement, for reasons of - pick whatever and reasons that we can't even think of right now because we're never going to get through them all.

You know, but the solution here is free consent of putting stuff in there because there are people who want their contact information in Whois, they want to be reached and many understand mail delivery and abuse concerns, all of this stuff and will put their information out there versus let's just lock it all down because the direction this is going and we all know it's going here, is doing what Go Daddy is doing and basically just shutting it down.

Chuck Gomes: So, John, you're jumping ahead to access, okay. I don't know that that helps us answer the question, what makes these purposes legitimate? And how do we determine whether a purpose is legitimate? Even with your suggestion…

((Crosstalk))

Chuck Gomes: …there's still the issue of whether certain data should be collected and if registrants give the right to access or have the ability to use privacy service to protect themselves, that's obviously getting into access and we can discuss that later. But how does it help us with regard to what makes a purpose legitimate for collecting data? I don't understand.

John Bambenek: If it's optional it doesn't matter. If I have the option of putting my phone number in there, right, it's Twitter. Twitter doesn't go through all of the possible uses of what information people can put in a tweet. I'm sure that if we got their data - data privacy analysis or impact assessment there isn't all of the possible things that you can put in there because it's infinite. If it's an option then, you know, we say we get the option of a phone number, what is the legitimate purpose, because some domain operators might want to have a phone number so that if I see a problem with their domain I have an out of band way of communicating with them.

If they don't want to put it in there, okay, that’s cool, then blank or not published or whatever, right? As far as I’m concerned we can throw out the whole proxy stuff and just RDS being not listed or information listed. You know, because all of that is essentially just another revenue stream anyway. Right? But if data is optional, then I don't think that an - we have to go through this exercise in the fine-grained painful detail in which we are because in essence if I’m putting something on my Website, I mean, if you're registering a domain inherently you want to communicate with the world, you don't need DNS to just run your own stuff, you need DNS because you want others to contact you.

Now granted, some people want to do that anonymously or any number of scenarios we can think of, right, but empower the users instead of us trying to figure out, you know, well do we need a phone number and decide in a globally consistent way because that’s absurd. Right? Tell the user, you have the option of putting your phone number in here. If you do so, it is available globally. There are reasons to do that, there are reasons not to do that; the choice is on you, the same way we treat users with Facebook and Twitter.

You can put pictures of yourself not wearing clothes on the Internet, but everybody in the world is going to see that. Some people want to do that, I don't know why, but it’s there. Right, it is on them and I think we should be more in the business of empowering consumers instead of shutting everything down and making all of these decisions on high for them because there’s no possible way that even - we even have proper geographic representation in this group to make that decision in a representative way for China or Asia or any number because I’m looking at the list of people and there's some pretty strong geographic bias of this working group.

Chuck Gomes: Thanks, John. So you would recommend making all data, except for the minimum public data set, optional?

John Bambenek: I would be cool with that approach.

Chuck Gomes: Okay, thanks. Stephanie, go ahead.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. I just want to raise the caveat that this is sounding blindingly close to the consent principle and that is much discredited in the current complex global environment. And I would suggest that ICANN's RDS is such an environment. It is almost impossible for a consumer who is not - or an end user who is not deeply embroiled in the DNS and how it works to understand potential use and pick up of their data. So I don't think that consent would work. And it involves a very, very high threshold of explaining to the consumer exactly what it means if you're going to put your cell phone, for instance, into the publicly available portion of RDS and you can't get it out and you're going to have pay the guys who run Whois - or Whowas, etcetera, etcetera, etcetera. So just a note of caution. Thanks.

Chuck Gomes: Thanks, Stephanie. Steve Metalitz.

Steve Metalitz: This is Steve. Let me just suggest one - at least possible way forward on some of these purposes for which there's either a sizeable minority or perhaps even a majority that says we think it is a legitimate purpose but there's a lot of people who think it isn't. I think you know, this gets back to the issue of - the first issue I raised about whether data that's collected for one purpose can be processed including disclosed for another purpose. Marika put in the chat part of what's ion GDPR about the test there being whether it's compatible - whether the second purpose is compatible with the first purpose.

There are some criteria by the way that say you can do it as long as it's not incompatible, which might not be the same thing. But the GDPR does give some guidance on this in Recital 50 and which - part of which, not all of which Marika put in the chat, and in Article 6.4. So maybe for something like - like for certification where we had a strong dissent we could conduct an analysis of whether that use, even if it's not a legitimate purpose for collection, would be compatible with a legitimate purpose for collection, perhaps using the criteria that are in GDPR Recital 50 and Article 6.4.

Nathalie has suggested, I think online that maybe we should have a small group look at this and try to come up with some criteria for what is and is not a compatible use and that might be helpful. But I think I just suggest this might be a way out for dealing with purposes that go beyond the inherent functionality test, perhaps, or at least some people think they do, and yet where there’s also a strong feeling that this should be available for processing.

And so maybe a focus on compatibility, for those that we don't - we decide are not a legitimate purpose for collection or many people think they're not a legitimate purpose for collection, we then look at the question of would processing of that data that’s being collected for another purpose be compatible with one of those legitimate purposes? Just a suggestion about how we might move forward.

Chuck Gomes: Thanks, Steve. I appreciate the constructive suggestion, we may come back to that. So John, go ahead. You're on mute, John. There we go.

John Bambenek: Sorry, I forgot. Yes, sorry, I forgot to take my hand down.

Chuck Gomes: Oh okay. Okay. Is there - how many of you would support, if you could just put a green check in the Adobe, Steve’s suggestion to form a small drafting team that would look at criteria for compatibility. Did I say that right, Steve? If I didn’t jump in. Or if you oppose it you can put a red X, do you think that might help us because we haven't made much progress today if any. So that sound like a good idea? Is there something else we need to do first? Criteria for compatibility is what the - is Steve the only one that thinks that might help us? What are the criteria for a purpose being compatible with a purpose for collecting data I think is what it is, Marika. Does that - did I say that right, Steve? Go ahead.

Steve Metalitz: That would look at - if we find - if we have a purpose that we don't think is legitimate or that many people don't think is legitimate should we then look at whether processing data collected for another purpose would be for that purpose would be compatible.

Chuck Gomes: Okay. Thanks. Anybody think it’s a bad idea? Okay, you can clear those checkmarks. So the next question is who would be willing to take a stab at that, be a part of that. Put a green checkmark now if you’d be willing to help on that task. If we don't have anybody to work on it, it doesn’t work. Okay, so Stephanie, Nathalie, anyone else? And Steve? Okay, Steve, would you be able to kind of facilitate online discussion with Stephanie and Nathalie on that in the next week? And just come back with some conclusions or recommendations for consideration by the working group.

Because we need to have a way forward and right now I don't see one jumping out at me. And so that would be really helpful. Steve, are you willing to - and all I’m asking is, is just kind of kick off the discussion with Stephanie and Nathalie and via email and if you need a phone call - need one set up you can ask staff and that can be facilitated. Is that - Steve, are you willing to do that? I see an “okay” okay. Yes, probably - it may take more but if next week you could at least give us a status of where you're at, I understand it may take a little bit longer, at least hopefully by next week can decide whether it looks like a fruitful direction. And then the leadership team will have to decide where we go next.

Our meeting next week is - I want to remind everybody is at the alternate time so please keep that in mind. Are there any other action items? I don't think we have anything for a poll this week but - and we’ll have to see what we have on the agenda for next week considering what’s transpired here. But the leadership team will consider that. I think our time is up so - or pretty close to being up so thanks for the participation today, we had a good turnout overall.

And we will let you know in terms of an agenda for next week and that'll be easier to do once the leadership team can regroup and look at all this.

Steve, yes, understand you might not be on the call but if you could send an email to the working group list just to give us a status update in terms of how it's going and whether it looks like a fruitful effort for the three of you and anybody else that wants to join you to work on that, that would be great. Okay? Thanks. All right, thanks, everyone. With that I'm going to adjourn the meeting and the recording can stop.

Julie Bisland: Thank you, Chuck. Today's meeting is adjourned. Everyone can disconnect your lines and (Princess), can you please stop recordings? Thank you.

END