ICANN Transcription

Thursday, 17 January 2019 at 13:30 UTC

EPDP on the Temporary Specification for gTLD Registration Data

F2F Meeting - Day 2

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

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

Kurt Pritz: So to start the day we're going to do some logistics discussions because people are changing their flights, afraid of the snow or something. It's okay, Alan, he's used to it. So we want to like do a schedule discussion since some people are leaving early and then a recap of yesterday and then we'll dive into the remainder of our work. So do you want to start?

Gina Bartlett: Sure. So I've heard from the Registrars that everybody needs to leave - that end of that table needs to leave around 3:00 tomorrow. Does anyone else have constraints tomorrow afternoon to leave early? Yes, what time? Before then or…

((Crosstalk))

Gina Bartlett: Okay. So your flight's at 10:00. So I think what we're thinking is that we will have, you know, the bulk of our work will stop by 3:00 but we may - since we have people here there may be some small group discussions where we can take advantage of folks' time together in person that we'll tackle after that but we'll try to have sort of a summation of where we're at and kind of some closure by 3:00 but then - and let's see how the day goes and I think by the end of the day we can sort of map out that bit for tomorrow. Does that sound good?

So any thoughts after sleeping and thinking about things? Any thoughts from yesterday and in a minute we'll review the agenda. Yes, Marc.

Marc Anderson: Thanks. This is - hello? Thanks. This is Marc Anderson. I don't know if this is for the agenda topic discussion or not but I'll throw this out there now. We recently got a memo from ICANN staff on, you know, it was a legal memo on the - I guess the contractual framework, and, you know, over breakfast a lot of us were talking and since we're all here and I don't see John Jefferies here but, you know, I understand he's here, if we could hear from him and have an opportunity to talk to him about the legal memo while we're all here in person I think that would be a great use of everybody's time. So we would like to request some agenda time, you know, if, you know, especially if John's available to talk about that.

Gina Bartlett: Great. And we have Recommendation 13, controller agreements which ties into that pretty well tomorrow morning on the agenda. Kurt or Marika or - Chris, were you going to say something?

Chris Disspain: Yes, I don't know - I'm assuming he's still here and I don't know when he's planning on leaving but if you want me to ping him and see if I can found out if he's happy to come and talk I'll do that and find out when he's going and I'll get back to you shortly.

Gina Bartlett: Any other general thoughts or ah-has or observations from your first day together, the first of so many? Yes, Diane.

Diane Plaut: We have discussed with Kurt - Diane Plaut for the record - we had discussed with Kurt the possibility taking up on James's suggestion that we put on the agenda some time tomorrow to discuss the format of the final report so that everybody could have the time to, you know, share thoughts on structure.

Gina Bartlett: Okay. Anything else? Okay. So what we're going to do today is we're going to tackle a suite of issues tied to, you know, maintaining security, stability and resilience through enabling of lawful access, Recommendation 2, the commitment to consider a system for standardized access to nonpublic registration data, Recommendation 4, 8, 9 and 12. These are all on your agenda. What we are proposing to do is to start with Purpose 2 and Recommendation 2, yes.

James Bladel: Sorry, our agenda's disappeared over here. And I know it's up on the screen but we also had some other packets that…

((Crosstalk))

Gina Bartlett: Right behind you.

James Bladel: Behind us. Thank you.

Gina Bartlett: Sure. We didn't want the caterers to pick those up and throw them away.

((Crosstalk))

Gina Bartlett: Okay, is everybody set? We're ready, okay. So we have this whole suite of issues and recommendations that we want to cover. Our proposal is that we start with Purpose 2 and Recommendation 2 and we have those two pieces together, okay? So I'm going to set this up and see where we go with this. I

know that this is a tough topic and you all have spent a lot of time on it. And it's been a challenge. So in Barcelona we spent most of the day on this and you had agreement to include Purpose 2 and Recommendation 2 in the initial report.

And so today we really want to spend some time thinking about what's changed, you know, what new perspectives have been offered through the public comment and then where do we go from here like what's the path forward. Right? So and I just want to honor that I think this is kind of the best and the hardest of some of the things you've done and when I say it's the "best" you have really collaborated on this because there's a lot of ambivalence about this purpose but you have put forward Purpose 2 in response to each other's interests, right?

You tried to find a path forward that said, okay, we can live with this. But there's a lot of ambivalence related to the processing aspect and the legal basis, right? Some people just don't feel that this is even necessary to have in there. And so I just want to honor that, you know, that you've done this and put this forward as a tool to collaborate with one another and then bring in the broader ICANN community and public to see and receive their comments and responses, and you got those.

So what I want to propose is that we start by having just individual time to think through our approach to this issue today. And I want to frame up a few questions for you to spend, you know, 5 or 10 minutes on your own to think through our approach to these issues because we've spent so much time, you know, talking about this; you've spent a great deal of your group time and I know that's also a source of frustration for some.

So the questions that I want to pose and we want to pose for you to think about are what are my interests? And what are my core interests? And what are others core interests with relationship to Purpose 2 and Recommendation 2. And then what do we need now and what's better managed in Phase 2?

Right? And Recommendation 2 I know speaks quite extensively to Phase 2. And then once you've thought about that, like what do I need, what are my interests, what would I like to see happen, I want you to look around the room and say, well how will others respond to this? Because remember we talked about yesterday we're trying to solve for everyone.

And how can I modify my approach, if needed, toward a path forward that you can all live with? And then when we get into the discussion in the large group I think what we want to talk about is, you know, what's changed? And how do we respond to new perspectives in the public comment and address the concerns and still have something that we call live with? And I think we think about the now and the Phase 2.

So - and I just drew this like diagram, I mean, it's kind of like concentric circles, you know, as you, you know, thinking about like what do I need, what does my organization need, what do we as stakeholders, what are our interests? How do we manage for the whole team in here because you are a microcosm, the real we're all here is your diverse perspectives. And then how do we manage the ICANN community and the public comment? So we're trying to like, you know, start with where we're at and work our way out.

So what I'd like to do is have Terri put 10 minutes on the clock and just 10 minute to think about these questions and think about how are we going to grapple with Purpose 2 and Recommendation 2 and then we'll open it up for conversation around what's changed and how do we respond to the new perspectives in the PCRT and address the concerns generally so that we can all live with the approach. Okay.

David Plumb: This is David. I'll just say again, our key documents are those summary tables and I'll make sure that everybody has them, right, Caitlin and Marika, the summary tables on Purpose 2 and Recommendation 2, so that's a good reference document.

Gina Bartlett: And then if you want more detail, the PCRT.

((Crosstalk))

Gina Bartlett: Put an hour on the clock and then we're going to check in.

((Crosstalk))

Gina Bartlett: …now and in Phase 2. (Unintelligible) kind of the high level before we dive into the (unintelligible).

Alan Greenberg: …others where it's in their domain then we need to make sure that they can get access as appropriate. If you look at examples like distributed denial of service, you know, that's not something we can fix ourselves; it breaks the Internet and we have to make sure that the processes are in place to make it work. We can keep going on but that's the summary.

Gina Bartlett: Thank you, Alan. Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. Basically we agree with what Kristina just said. We have made this point repeatedly, just as, you know, a bank does not have to state the - a purpose of, you know, making sure that funds are not stolen and that crime doesn't reign in the banking environment, ICANN as the custodians of the DNS system, they don't have to state that they're collecting information for the purpose of disclosure to bona fide actors who are investigating potential fraud. So we would like to see it deleted and we would also like to hear from legal counsel, now that we have her, what the views on this might be. Thanks.

Gina Bartlett: Thank you, Stephanie. Kavouss.

Kavouss Arasteh: Thank you. Good morning to everybody. We, to GAC member, have been in a discussion together. We think that there is some sort of nuance here. We

indirectly invoked something that the mission of the ICANN in Bylaw would be maintained to access to this legitimate right to so on so forth.

That is not the case. The case here we are talking to provide or enable access to the third party interest while maintaining or doing anything on this regard should be in full consistent with the bylaw. I don't know, we are just trying to say that bylaw may need to have some change. This is not the purpose.

I don't think that the purpose has been written properly. The staff should not be (unintelligible) maintaining - maybe consistent with the ICANN bylaw, ICANN mission in the bylaw, then you do whatever you want here. But now you changing the directions of the discussions and changing the maintaining ensure, I don't think that they applied the issue. This access would not ensure the stability and so on. Access should not have any impact on the stability, resilience and security of the DNS.

So we need to look at the preamble where we start; we start from maintaining the stability and so on so forth or we start to provide access consistent with the ICANN bylaw for maintaining or ensuring the stability and resiliency. Look at this structure of the sentence; there are some weakness, there are some problem there. Thank you.

Gina Bartlett: Thank you, Kavouss. I've got Mark, James and Benedict.

Mark Svancarek: Mark Svancarek for the record. I'd like to address some of the earlier comments, okay. I'd like to address some of the earlier comments. As Alan has stated, we really aren't just collecting this data for the purpose of disclosing it but certainly GDPR does not prevent us from processing data. So if we have a purpose in disclosing it, that should be allowed so long as we state that purpose up front at the time of collection, that we are collecting this data for these following purposes.

We think that this purpose as stated, would benefit from a little bit more specificity; it originally was more specific. It might even be broken into a Part 4, law enforcement and a Part 4, civil purposes as well.

But as you see in the public comments, there is a list of reasons why this data should be disclosed; those are true reasons, justifiable and we believe that as long as they are disclosed at the time of collection that this is perfectly allowable under GDPR.

Gina Bartlett: Thank you, Mark. James.

James Bladel: Thanks, Gina. James speaking for the record. And on behalf of the Registrar delegation, I think just for brevity our position is very clearly aligned with what Kristina laid out for the Registries. And as the other contracted party with ICANN we see that this purpose is not explicitly contained within the mission of ICANN and this is an ICANN purpose but it's written as though it's a third party - a purpose for third parties and third party access to the data.

I think that if we could get some clarity both from our legal advisors on this point but also from ICANN Org on their establishment of this purpose as a part of their mission, I think that would perhaps be a start towards helping us close some of these gaps but I think right now we're kind of staring at each other across the chasm as you can see from our comments, our stakeholders were pretty consistent that this needs to be deleted.

Gina Bartlett: Thank you. So I think I'm going to hear from each group and then we will - I'm just putting the legal counsel on notice that we're coming your way. So I've got Benedict next - I've got Benedict, Hadia, Thomas and then we will be headed over there to the legal counsel.

Kurt Pritz: Haven't you heard from ALAC already?

Gina Bartlett: Oh and IPC - okay.

Benedict Addis: High five. I'm not going to bore you with restating any arguments. We live in a weird ecosystem and to Stephanie's point, in a normal ecosystem ICANN and the contracted parties would be responsible under Recital 49 for their own network security and they'd be allowed to do their own investigations and get their own data and that wouldn't need to be a stated purpose. But we don't live in a normal ecosystem; we live in a place where random third parties, odd people, huge corporations, and everyone in between, is responsible for the security of the ecosystem we all operate in.

So the reason we, as I remember, that we put this purpose in the first place was to explicitly explain to the data subject, the person that we have to explain this to, why we are sharing their data out with the ecosystem and out with contracts. So if we don't think this should be in here, then we need to think about what replaces that.

And, you know, a system of contract, a system where ICANN is explicitly contracting with people or has relationships with the people doing this kind of work, but at the moment we all rely on this very nebulous relationship with the people doing the cleanup and doing the investigations and the organization relying on it and that's why this is in there, this particular purpose. Thanks.

Gina Bartlett: Hadia, you put your card down, so Thomas.

Hadia Elminiawi: Hadia Elminiawi for the record. So my comment was very much in line with what Benedict said. So we heard from the Registries and Registrars two points. The first is that the data - no data should be collected for this purpose and actually the purpose explicitly says that the data is - the data collected for the other purposes is going to be disclosed, so no data is collected for this purpose. Second, with regard to the mission, you know, is it an ICANN purpose or not, the disclosure. And I guess we're going to hear from the legal people about that.

Gina Bartlett: Thomas.

Thomas Rickert: Thanks very much. Now this very purpose has been discussed quite heatedly inside the ISPCP. And unfortunately there was no box we could tick in order to accurately reflect the views. So it's not like the ISPs reject the notion of honoring lawful disclosure requests, so if there is confirmation that the purpose, as written, is sustainable, a lot of the concerns would be put at rest. But let me try to explain what the issues with Purpose 2, as we see it today, are.

And you might remember that when we discussed Purpose 2 in Los Angeles, at least my understanding was that we would keep it sort of as a placeholder to have something in there for those who are interested in disclosure - the disclosure debate so that the whole access discussion, the disclosure discussion is not swept under the carpet. But it was always my impression that Purpose 2 would need to be refined as soon as we discussed the various disclosure scenarios and then see which ones are lawful and should be reflected and which were - are not.

The purpose, as written now, says that the contracted parties and ICANN should keep data just in case somebody asks. And we don't know who's going to ask and what they might need the data for. And one issue is that we are lumping all requestors into one sentence without specifying who it is. So this talks about legitimate third party interests; that suggests we're talking about a 6.1(f) processing. But 6.1(f) is blocked for public authorities in performing their core functions, so they have to go through 6.1.(c) for example.

And so I think we need to be far more nuanced in this, look at who's asking, you know, GDPR makes it relatively easy to honor disclosure requests when it comes to pursuing civil claims. It's different for law enforcement because law enforcement is much more impactful on the data subject because they can investigate people, they convict people, they can put them behind bars.

And so I think what we should probably do in order to get - to move forward with this is hear Ruth's views, maybe she said this is all fine and that would make us reconsider certainly.

But other than that I think we should discuss who is the requestor; is it law enforcement, is it a civil actor? What claims are they pursuing, then conduct the balancing of interests and in those cases we can confirm that a disclosure request can be honored. I think we need to probably come up with a couple of purposes replacing the current Purpose 2 and make that explicitly clear so that the data subject has clarity on - under what circumstances data might be revealed.

The other issue is that we have the word "access" in there and I think that access is a concept that is not really embedded in the GDPR. So GDPR, you know, looks at a case by case handling of disclosure requests. Access suggests that somebody can self-serve and I'm not sure whether that's something that we can do. But maybe Ruth has some views on that as well. So it's multilayered, I think probably the best we can do in this session is to agree on a path to creating the scenarios under which disclosure would be lawful and then revisit the language of the purposes.

Gina Bartlett: So, Thomas, can I just ask a follow? I mean, is - some of what you're talking about, is that a now activity or a Phase 2 activity?

Thomas Rickert: I think it depends on how far we get in this discussion. There are some low hanging fruits; I think you know, for example civil claims are much easier to handle than law enforcement requests because - and we haven't even talked about who the requestor is. It's a different thing if European law enforcement asks a domestic contracted party versus a non-European law enforcement authority asking. And so I think we really need to go through the various cases that might occur…

Gina Bartlett: Okay.

Thomas Rickert: And then specify the purposes accordingly. But maybe Ruth gives us an easier way out of all of this.

Gina Bartlett: So I see Stephanie and Alan…

Thomas Rickert: No pressure.

Gina Bartlett: But we haven't heard from IPC so my proposal is let's hear from IPC and then let's go to Ruth because a lot of you, including you, Stephanie, have framed up questions for Ruth. So go ahead, Diane, and then we'll go to Ruth.

Diane Plaut: Yes, thank you, Gina. As Gina explained and started out this discussion I think really importantly this morning we've all come so far; we've spent so much time on this in LA, in Barcelona, and we've been, you know, really committed to trying to be thoughtful in our work. So we've discussed the fact at the bylaws support a framework like this; we've discussed - we've gone through all the work of assessing the data elements, the legal bases, and we've set up a purpose here that aligns with a 6.1(f) under GDPR. It is supported by this and by the ICANN framework and as it exists today by having law disclosure requests whether it be on a law enforcement basis or on a civil basis.

Whether this purpose now needs to be separated out, as Thomas and I have - and we have discussed offline, but it's highly important and practical for us to maintain this purpose because it really is supporting a system that already exists but then applying the GDPR as we're meant to do under this EPDP. So we might need to break it down here and we might need to actually synthesize to make clear the legitimate interests of the various third parties into different purposes, one for law enforcement, one which takes into account language saying that any needed additional information from local laws is required, and then one that breaks it down into the various elements

that we've discussed are already in the bylaws of ICANN. So that is the IPC firmly supports that position.

Gina Bartlett: So Ruth, I think you've heard, I mean, we could try to restate but I mean, I think you've heard the, you know, is it necessary, you know, that GDPR doesn't prevent, there are a whole suite of issues there so - and we've talked about it a little bit this morning. So could maybe we just hand the mic to you and hear your insights and thoughts on some of these key questions?

Ruth Boardman: Sure. So first of all thank you for organizing the comments to share them just now; that was really helpful. Secondly, is there an easy way out? Well if there was I'm confident you would have found it and you wouldn't be asking the question. I thought it might be helpful to share or to structure my comments around three points. The first is about reactive disclosure and whether you need this purpose to facilitate that.

And there - I should preface all of this by saying that it would probably be helpful for me to confirm this in writing because if you speak - if I speak off the cuff and inevitably I will miss some of the detail when you firm things up in writing, you make crisper points and it avoids missing points that would be helpful. So I'm very happy to share immediate reactions but I would like the opportunity to do something more considered because I think that will be helpful for you and for me.

So the first point, do you need this purpose in order to ensure that registrars can respond to appropriate request for personal data? I think the answer to that is no. It is clear that if a controller has personal data for the purposes of running its business and it receives a request from a third party who is entitled to or where you are able to disclose the data under the principles in 6.1, then you can do that; I don't think you need this purpose to make that possible or legitimate.

I think the points Thomas made that legitimate interests are not the only condition under Article 6 is a good point. Article 6.1(f), so legitimate interests, the provision that allows you to share data with a third party where that third party has an appropriate interest and where the interests of the individual don't outweigh, that's the obvious condition to look to. It's the condition that the European Data Protection Board has pointed out, there is case law and (unintelligible) case that suggests that it's an appropriate condition.

But I think Thomas's point is spot-on that that won't cover all third parties so that will be something that will be worth looking into I think to ensure that disclosures that could be permitted under a different condition can also be accommodated. So just to recap on that, the first point, could registrars and others disclose in appropriate circumstances without this condition, I would say yes, absolutely.

The second point, do you have to explain this to individuals? There were a number of comments, I think Stephanie, you picked up on that, well - yes. And this does have to be clear to individuals. A controller has to make clear under Article 13 and 14 so the articles which require controllers to explain the purposes and other material facts about their processing. Under those conditions you also have to inform individuals about the recipients or categories of recipients of the data. And if we are aware that that will include rights holders, organizations involved in proceedings, law enforcement authorities, then that information ought to be included.

When you look at what happens in other sectors, I know Stephanie, you mentioned financial service providers will typically in their privacy notices, they do explain that they will share data in appropriate circumstances with those kinds of organizations. So that would be the second point.

The third point is could registrars and others have a purpose of collecting data in order to disclose it or could disclosure be a purpose in its own right? There was some discussion as to whether that was at all possible under

GDPR. To my mind GDPR doesn't stop you from doing that. If your purpose as an organization is to share data, then that is your purpose and there are certainly organizations who do that.

So if you look at organizations who collect data to provide information about individuals who are suspected of money laundering events or who appear on sanctions lists, their purpose is to collect data in order to license it to third parties or to make it available. So - and I can see some critical faces so this might be one to discuss.

But as a matter of principle I don't see why GDPR stops you from having a purpose which is to collect data in order to make it available to people. It seems to me that there is a policy question which is, is this the purpose for which registrars and others are collecting data? And it seems to me that's not a - that's a question where you don't find the answer in GDPR; it's a question to be resolved as a matter of policy in probably in this forum.

And then there was one question which I think I've not answered which was, is this a purpose for ICANN? And I don't feel I can answer that question because that's really not a data protection question, it's a matter of what ICANN's own mission is.

David Plumb: Great. Okay.

Ruth Boardman: I might stop there and there'll probably be lots of disagreement and comments back.

David Plumb: Great, okay. Gina, you want me to handle the queue and - okay. So clearly there's going to be a lot of comments and questions and I think this is an opportunity to do a little of that with the caveat, as Ruth says, that you'd prefer also to write some things down here. Okay. Great, let's jump to the cards. I know, Stephanie, you had your hand up even before Ruth. We'll go to Stephanie, then Milton, I don't know…

((Crosstalk))

Gina Bartlett: …been up too.

David Plumb: …Stephanie, Alan, then I'm going to go down the row and we'll make it - yes.

Stephanie Perrin: Stephanie Perrin for the record. Thank you very much, Ruth, I think that as a very good explanation. And that fundamental policy question is haunting us I think. I raised my flag earlier to respond to Benedict and to which, you noted in your exposition of the points, there is a conflation I think in our discussion on this point between what you have to do in terms of transparency to the end user, to the registrant, and a purpose. So you know, I think you touched on this but just to be crystal clear, the way I read it, you do have to be transparent to the user but the potential recipients, that doesn't mean you need a purpose that outlines all of the potential ad hoc disclosures. So I see you nodding for the record, that's good.

Now second point, to respond to Benedict, for whom I have deep sympathy even though I've spent much of my career fighting with law enforcement about the procedures they have to follow in order to get personal data, we recognize there is an (unintelligible) environment for the policing of cyber crime. The GDPR should, in my view, be a trigger to try to put some order in that.

That and I would draw everyone's attention to the 2012 memo that we received during the negotiation of the 2013 Registrars Accreditation Agreement, from Jacob Kohnstamm who was the head of the Article 29 Working Party at the time, and he was referring specifically to the data retention clauses that we were bringing saying basically if countries wished ICANN to become a repository for data for the purposes of law enforcement, then they should legislate but it was not up to ICANN to do this.

Now, I recognize that what Benedict's talking about was not data retention for those purposes but it's all much of a muchness in terms of what we're talking about here. If ICANN is to state as one of its purposes that it will gather data for the purposes of any kind of law enforcement action, then it is really operating in a way that is somewhat extraordinary. And I think the - a good analogy to what Ruth's final point was in terms of that policy question, we do have credit reporting agencies in many of our countries and usually they're legislated as to what they can do, what data they can do.

I'm certainly very familiar with the situation in Canada. There's mission creep all the time, where now your credit score can be used to determine what you pay for your house insurance. But, you know, there are controls that are legislated. And so the question to me is how much of a license does ICANN think it has globally to set this up. I'd rather see data processing agreements put in place myself. Thanks.

David Plumb: Thanks. Let's go to Alan Greenberg.

Alan Greenberg: Thank you. Alan Greenberg speaking. I guess if we don't need a purpose to do all of this, and we can still do it and do it well, that's fine. I have a lot of concerns, a lot of what Stephanie was talking about was law enforcement; we're not talking about law enforcement here. We've always presumed that law enforcement was under a different clause and was not - and - Benedict, you're the one who said it's not under 1(f), it's under something else. No, okay. In any case…

((Crosstalk))

Alan Greenberg: …in addition to law enforcement, there's a whole civilian corporate cyber security force essentially that works to try to keep the Internet safe and proper. I have a great concern saying that any contracted party could release information under the right rule, under the - under good circumstances without a specific purpose, without referencing one of James's companies, I

think that becomes the wild west where we have, you know, hundreds or thousands of contracted parties working under their own rules without any uniformity, without any coordination, without any - I'll use the word purpose - without any cohesiveness to how they're doing it and the purpose for which they are doing it. And I don't think that's sustainable. Thank you.

David Plumb: Thanks. All right I'm just going to say what I have on my list, Milton, then Benedict, then Kavouss, then Chris, then Kristina, then Mark, then Margie, all right. It might not be perfect order but it's what I got. And then James, okay, so Milton, you're up.

Milton Mueller: Okay, so this is Milton Mueller. And James, I think, said that we were staring at each other across a chasm and I actually don't think that's correct. I think the - it's a step; it's a very small step that people have to take. Unfortunately I think the people who support Purpose 2 have gotten it into their hearts that they have to have this or they're not going to get access. We just heard a bit of that from Alan, at the same time he started out by saying the correct thing which is you don't actually need this purpose to have a system of access.

Now if you don't recall, I think I was the one who sort of framed Purpose 2 as a compromise in Los Angeles. And we thought that that would do the trick because it made it clear that not additional data was going to be collected. But then after reading the public comments, it became clear that this just doesn't work logically for the legal reasons I think that Ruth has outlined and that it became even clearer after we passed - or we will pass Recommendation 2 that we've committed ourselves to developing a system of access that what exactly do we need this purpose, which doesn't make any sense on its own terms, why do we need this? What we need is to get over with the temp spec and get into a system of access.

And if you read all of the comments in favor of Purpose 2 in the public record, they're all saying we want access, we want access, we want access, that's all they're saying. And so the assumption is if you don't have this purpose you're

not going to get access. How can the possibly be true? We have Recommendation 2, we have some other recommendation in there that is basically committing ourselves even before the temp spec expires to flushing out the conditions of access to making them more uniform.

So why, you know, I know it's a big step but I don't think any of you will ever be able to convince me that if you don't have Purpose 2 there will never be lawful disclosure of Whois data to anybody for any legitimate third party reason; I just think that's a false premise. And so we can take that step, which is not a chasm, it's just like a little crevice, and I think we can move on.

David Plumb: Thanks. Benedict, you're up. And let's try to be extremely brief just like Milton was, thanks.

Benedict Addis: Okay, brief. Your point 1 you said - I think I understood you to say that no purpose was needed for disclosure, I think you said reactive disclosure, by a registrar. And I think we can extend that to mean registrar, registries, the individual players. But that's not what we're talking about here. I think we understand that within a particular legal system, within a particular country those organizations are bound to respond to requests within the framework of that legal system.

The reason we felt it necessary to have a purpose was to define a unified access system, mandated by the ICANN community and implemented by the ICANN organization. That's the sort of logical step that we're doing. We all decide that we want a thing, it sounds like maybe some people don't, but then we ask the ICANN organization to be party to that - that contract and to have that information collected so that it be available for on the disclosure.

My question is, and this is something I've been struggling with, if such a system is legally possible, is the data to be collected - is it adequate to use legitimate interest to collect that data even if a public body is then requesting it? And will the - and so if a public body is requesting that data that has been

collected under 6.1(f), is that adequate and will the public body then rely on 6.1, I believe, (c) in order to access it?

In other words, are there two steps to this process? And the secondary question, if there's a secondary step - if there is a second step, does that then bring the data supplicants, the people seeking this data, whether that's intellectual property rights holders, law enforcement, or others, does that then bring them into a liability - the liability realm of GDPR? Does that perhaps make them a controller? So if they're regularly requesting data that has been previously collected, would that make them a controller?

Ruth Boardman: Could I just…

David Plumb: yes.

Ruth Boardman: Sorry, could you just run that last point - could you repeat that one so that I know from whose perspective you're asking the question.

Benedict Addis: So we are - the question presumes something that we haven't agreed on, I hope that's okay, that we have an access system mandated by ICANN where ICANN has asked its contracted parties for data to be collected for this purpose. Right? Again, we're in an unusual ecosystem. ICANN isn't collecting the data itself, it's requesting that others do so to fulfill this purpose, that's the point of this purpose, right? There's then a data store that's some sort of retention of data. Requesting parties then go through a gated system to request access to that data. So what legal basis would that likely happen under?

And secondarily - second question, would they be then responsible or would they be liable under GDPR and brought into the GDPR purview, if you like, as a controller or possibly another designation? Is that clear now? Thank you.

David Plumb: Ruth, if you want to sit on that; you don't need to answer that right now. I think maybe we'll do a circle of comments and come back, yes. Okay great. So I have on my list Kavouss and then Chris. Kavouss, you're up. And don't forget to state your name, folks, for the record. Thanks.

Kavouss Arasteh: Thank you. No problem. I come back to what I said before, the sentence is transgressed. We should start with something that does not have any impact on the current ICANN mission in the bylaw either at the beginning, we should say while ensuring or maintaining stability and so on so forth, and then saying for enabling access and continue the situations. Otherwise it should be understood that this providing access is to maintain the stability and resiliency and security of the domain name system. That is already there.

If we provide access, this access should be consistent with that mission and does not modify that mission at all. So we have to properly describe the situation and reword them if you want to but I have no problem to change maintain by ensure. I have no problem to describe what is the legitimate interest of the third party as law enforcement and so on so forth, no problem at all with any of them.

But the beginning of the sentence should be correct, either starting while maintaining or ensuring and continue or the two other alternatives I have provided in the chat. I have serious problem if you start the sentence, maintaining or ensuring, it means that the current mission of the bylaw requires to be reinforced by providing access to the third party; that is not the case. Thank you.

David Plumb: Thanks, Kavouss. Chris.

Chris Disspain: Thank you. I want to address very specific - and I've just sent an email to the list and I've copied to Ruth. I want to read the attachment because I think it's important it gets read into the record so I want to address the concept that this is - that third party access is outside of ICANN's mission.

“ICANN’s mission” - and I apologize, I’m reading it but I think it’s important. “ICANN’s mission is clearly stated in the bylaws. In summary and with respect to names, ICANN is responsible for developing and implementing policies relating to root zone assignments and second level registrations in gTLDs, for the purpose of ensuring the stable and secure operation of the Internet’s unique identifiers. It’s required to limit itself to issues requiring uniform coordinated approach. It’s reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the Internet and the DNS and it’s got to do that through the bottom up process.”

“Certain things specified in the annexes are by definition, within ICANN's mission meaning that coordinated policy is reasonably necessary to ensure SSR. The referenced annexes specifically describe maintenance of and access to accurate and up to date information concerning domain name registrations, as an example of the topics, issues, policies, procedures and principles referenced in Section 1.1.(a).1 of the bylaws for the purpose of ensuring the stable and secure operation of the Internet’s unique identifiers.”

“And the annexes specifically reference policies regarding the resolution of disputes regarding the registration of domain names, as opposed to the use of such domain names but including where such policies take into account the use of domain names. This purpose encompasses not only dispute resolution processes like the UDRP but access to registration data by third parties for the purposes of dispute resolution.”

The note that I've sent has that text in it plus a little bit more plus a whole series of footnotes and references to the bylaws. Those who state that it is not within ICANN's mission, I would ask you to be very clear and explain why you don't think it’s in ICANN's mission; it seems to me to be patently obvious that it is. It says so in the bylaws and therefore it is within the picket fence and therefore it’s something that we should be having policy on. Thanks.

David Plumb: Thanks, Chris. Kristina, you're next.

Kristina Rosette: Thanks. First of all, thank you very much; I thought that was really helpful. The - your answer I think covered a lot of the sub points that we've been discussing for quite some time, and I think added some additional clarity that we hadn't had. It's kind of fortuitous that my question follows Chris's intervention because the question that I had for you was I was very interested in getting some more information about the point that you made that some organizations do have a purpose of collecting data for the purpose of disclosing it.

And just to the extent that you can elaborate on are there particular criteria that must be met in order for an organization to say, yes, this is our purpose? For example, is the articulation that Chris just made, would that be sufficient? And if not, what else would we need?

David Plumb: Thanks, Kristina. Let's just keep rolling through and then we'll - as long as you're taking notes, Ruth, for this extensive round of comments. I've got Mark and then Margie and then James. Okay so Mark, you're up.

Mark Svancarek: Yes, Mark Svancarek. So my question is whether - we recognize that the contracted parties could respond to lawful requests for third parties for legitimate purposes. But we would like to ensure that ICANN has the ability to enforce such disclosure in a consistent manner, a consistent and unified manner. And so we had thought that having this purpose - an ICANN purpose, not a registry or registrar purpose - we had considered that having this purpose would allow ICANN to create contracts and to enforce them to ensure that this disclosure was consistent and reliable and timely.

And so our question is, is this purpose required for that? And does it benefit us in any way to have this purpose to avoid, you know, ad hoc disclosures with all sorts of random parameters?

David Plumb: Great. Thanks, Mark. Margie, do you want to build on that?

Margie Milam: Sure. This is Margie. The other thing I wanted to point out - I agree with, obviously what Mark said - is that we're building a global policy here so although, you know, we appreciate Ruth's note that maybe this, you know, that you could still provide access under GDPR if you didn't have this purpose, that doesn't address the, you know, how we provide the access for these purposes for areas outside of the EU that are covered by GDPR. And so what we really want to do is ensure that we have a policy that's consistent across the globe that enables access for the things that we all recognize are important and are things that we thought were addressed in our early negotiations.

I mean, part of why you're seeing some of the reaction is that, you know, we negotiated to get to this point and we're obviously certainly happy to go back to, as Thomas said, more specific purposes relating to the different interests and that's certainly on the table and I'd like to see if that's some way we could explore those concepts because in our view if, you know, the group is no longer interested in Purpose 2, then let's go back to the specificity where we started from back in Los Angeles. Thank you.

David Plumb: James, you're up.

James Bladel: Thanks. James speaking. And I think I put my card up ages ago in response to - I know, it's the nature of the beast, but I think I wanted to respond to just some comments or maybe, you know, explicit or implied by Alan and by Benedict, and maybe they were just kind of throw-away statements regarding contracted parties' willingness to cooperate or disclose information in response to things like law enforcement, online crime, cyber security and things.

And I just want to be very clear here, particularly because we have, well, we had two Board members in the room, now we have one, to be very clear here

that this is not a question of wanting to disclose information to those types of authorities. We want to ensure that we have the cover to do so; we want to ensure that we have the legitimacy to do so. And I don't even think that that's an issue in civil concerns; I think there's a consistency problem. I think cyber security poses a bit of a challenge because to Alan's point, there is this civil force keeping the Internet safe.

Well, somebody needs to tell us who the good guys are and who the bad guys are because the bad guys think they're doing cyber security too. So, you know, somebody needs to sift that out for us. But I just want to make sure that we're understanding before, in order for us to make progress on this issue and this purpose, we have to establish - I don't want to say we can't get tied up into narratives and the narrative that contracted parties don't want to do something is just simply not correct. Thanks.

David Plumb: James, can I quickly bounce back to you and ask you to respond directly to some of the suggestions like what Mark said, like this purpose is about creating some consistency and some standardization? Could you respond to that particular…

((Crosstalk))

James Bladel: So I think we're starting to stray into the access discussion and these are very tricky problems and I would hope that the follow on work would sort them out. I will say that at the high level there is this dichotomy between we know the scale we're dealing with. We can't have an army of people reviewing these types of requests, you know, we can't hire 10,000 lawyers to go through them. On the other hand, we can't make one mistake, so we can't programmatically just allow a process where input XY and Z yields output AB and C.

So I understand their desire for consistency and their desire for programmatic reliability and kind of a deterministic process that they can rely on but I also

think that from our perspective there has to be some discretion and review in that process, so I think that's a challenge but I think that is, I mean, hopefully we'll all be retired and the poor souls that have to pick up Phase 2 will have to wrestle with that one, and I know it's going to be us. I'm just kidding. But it is a challenge and I think that's one of the overarching issues that's going to have to be solved in that group.

David Plumb: Hadia, you're next. Oh sorry, Diane was actually next and then Hadia. Sorry about that. Diane, why don't you jump in and then Hadia.

Diane Plaut: Sure. Thank you. Much to what Chris stated and put forward in his email, it's clearly within the bylaws of ICANN to have this purpose. Ruth has expressed that this is not a traditional context right here; we're in a multiparty stakeholder community and universe and because of this there's reason for this EPDP having formulated policy that provides clarity and application of the GDPR.

And so while this purpose may not be 100% needed, the point is, is it advisable? Because our mission here is to provide clarity and application and even as James has just explained, there is a lack of clarity on how to apply. And it would almost make it much easier and provide for policy going forward that lays the foundation and the basis to have a definite policy that is clear in providing a foundational way to go forward with any type of unified access model or any kind of reasonable access - a recommendation or purpose that's otherwise put forward in this policy. So really having this lays the foundation for everyone in this room.

David Plumb: Thanks, Diane. Hadia, then I've got Stephanie, Chris, and then I'll circle back to Milton and then we're almost out of time and we want to make sure Ruth has some opportunity to respond to a lot of these questions. Oh I see Thomas put his hand up too. Hadia, you're up.

Hadia Elminiawi: Hadia Elminiawi for the transcript. So according to Chris, definitely this purpose is an ICANN purpose and following on what Margie and Mark said, the reason we were looking forward to have this purpose is to ensure that we have this kind of standardized system in which disclosure could be possible through it. However, this is not why I put my card up. So I put my card up to ask the Non Commercial Stakeholder Group and the contracted parties, so if we actually don't have this purpose, if we agree or decide on removing it, would you be open to having a paragraph in the report that speaks about disclosure of data and a standardized access system or model spelling out the purposes and the legitimate interests that could be involved with that?

So if we decide to just remove this purpose, because actually we could actually disclose data without having this purpose, would you be open to having a clause or a paragraph that speaks about disclosure and a standardized system in the initial report as a consensus thing that we all agreed on?

((Crosstalk))

Hadia Elminiawi: No, but what's in Recommendation 2 it's only like two, three lines that only speak about the - that we are going to be addressing the issue of standardized access, but it's not enough. If we are not having this purpose then Recommendation 2 is definitely not enough. We need to have a clause or a paragraph that it's more specific than just saying, you know, we are going to address standardized access in the second phase.

David Plumb: Thanks, Hadia. That's helpful. Stephanie, you're up.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. Maybe I should respond to Hadia rather quickly. Absolutely. In response to what Chris said, nobody's arguing that ICANN doesn't have in its mission the security and stability and all the rest of it; however, that doesn't mean that it needs to be stating, as a purpose for data protection purposes under the GDPR, disclosure like a credit

reporting agency, for instance, its sole purpose is to act as a reference point and disclose information about people's credit history, right?

Nothing precludes ICANN in its mission setting up a standardized access system, in fact the Non Commercial Stakeholder Group does not want to price domain names out of the market by - as I think James said, you know, hiring - I can't remember whether it was James or Kristina - hiring, you know, 85,000 lawyers to look at every request. We want a smooth, streamlined system where there are protocols and that's why some of us are busy working on a data trust model.

So that I think should answer your concerns, Hadia. Nothing - you don't have to have this as a purpose in order for ICANN to work on a standardized access model. However, and this is why I raised my flag, I forgot to mention in my earlier remarks that one of the objections we have to stating the disclosure of data as a purpose for law enforcement and other investigations, is then that more or less opens up the gate on the data elements question because there are governments for instance already like to get a retinal scan of individuals to do secure authentication. And I know there are probably folks in this room who would heartily agree with that.

However, we as the Non Commercial Stakeholder Group don't think you should have to do a DNA sample to get a domain name; we want to keep this open and free and transparent but not (surveillant). Thank you.

David Plumb: Thanks. Chris, you're up next.

Chris Disspain: Thank you. And thanks, everybody, for this debate which I think is really interesting. Stephanie, with real respect I think you're wrong; I think if it's not in ICANN's mission, ICANN simply can't do it.

David Plumb: Purpose, you mean if it's not a stated purpose…

Chris Disspain: Well if it's- I mean, in its mission, so let me explain where I'm at with this. And I want to stress I am speaking personally although I suspect that a number of my Board colleagues might agree with me. I think Mark is right. Mark said this is all about whether ICANN can provide access or make sure that access is provided to legitimate third parties. And in essence it seems to me it needs to be an ICANN purpose so that ICANN can enforce access by third parties. And ICANN can't make registrars or whoever has the data provide that access unless it is a purpose.

I can't see any other way in which ICANN can do that unless it's a purpose. It doesn't have the power to make registrars do stuff unless it's policy and therefore it's got to be in the policy and if it's in the policy there needs to be the purpose, otherwise it just doesn't hang together. And my view is, so if you want to have a meta-discussion about whether it is in the bylaws or not, whether in fact is in ICANN's mission to do this, that is a discussion to have. But if you accept that it is in ICANN's mission to do it, then my view is there has to be a purpose, otherwise it's not within the picket fence; it cannot be dealt with and you can't make policy on it and ICANN can't enforce it.

So if you want a situation where the data is collected by the registrars and is kept by the registrars and only the registrars get to decide who has access to that data, then you would set a policy that has no purpose for ICANN in respect to the data. But if you believe that it is ICANN - in ICANN's mission and it is ICANN's mission to, amongst other things, provide this - or make sure this access is provided, then it needs to be in there as a purpose.

David Plumb: Thanks, Chris. And this seems like a really core question that Ruth can help us with. I've got Milton and Thomas and then we're going to turn it back to Ruth and then we're probably going to take a break and see where we are. Milton, you're up. Thanks.

Milton Mueller: Okay, try to be brief, but I'm basically reacting to Chris's erroneous and illogical argument that because it's in the mission, security, stability and

resiliency is in the mission therefore we need to define collection for the purpose of disclosure as a purpose; that's a complete non sequitur. What he's saying in effect is that ICANN has no authority to require registrars to disclose data under terms and conditions that are standardized unless we define this as a purpose? That's completely a non sequitur. That doesn't make any sense at all.

Standardized access is a policy. The reason we're in this situation today is that we had no access policy, we had open indiscriminate disclosure, right? And that was imposed on the registrars by ICANN. All we have to do now is have a policy for disclosure that is GDPR-compliant or privacy law-compliant. And in order to do that it actually hurts compliance with GDPR to have this purpose because it's so indiscriminate, it doesn't say who gets access, when for what reason, and if you start trying to make it more specific, Diane, then you're actually defining the access terms and conditions in a purpose rather than actually having a purpose.

So it's just a ball of worms that we just don't need to get into. We don't need it as a purpose, we have committed ourselves in Rec 2 to have a standardized access mechanism and the longer we get stuck on this purpose problem, the less time we will have to develop a standardized access mechanism that can actually solve the problems that we're debating. So please don't get mixed up with mission, purpose and policy; we…

((Crosstalk))

Milton Mueller: …and accreditation agreements and so on are all mechanisms by which ICANN can enforce an access policy whether you have Purpose 2 or not; it doesn't make any difference.

David Plumb: So in the interest of time, I'm going to stick to my old queue of just going to Thomas. And I see that Chris wants to jump back in and Alan wants to jump in. And I wonder if we can just hold it now to Thomas, go to Ruth, right, and

see where we are and probably take a break if - Alan if that's okay? Yes. So Milton, you get the last word in here before we jump back into Ruth and then we'll come back in. Thomas, sorry, excuse me.

Thomas Rickert: I take it as a compliment if you confuse me with Milton. I think what we should probably do in our final report is get some definitions and terminology clear because I think that we're conflating different issues over and over again. So the reason why we have this list of purposes is because the European Data Protection Board or at the time the Article 29 group asked ICANN not to conflate its own interests with third party interests. So we wanted to get clarity on who is interested in what, whether it's technically a purpose that's required or not, but we wanted to get clarity in whose interest are certain things happening. And so I think that needs to be clarified.

Also, the term "ICANN purpose" is misleading and I think we only have a footnote in one of the worksheets in our report clarifying this. It is not a purpose exclusively limited to ICANN but it is a purpose that ICANN should enforce because we're talking about policy that ICANN via contract can enforce. And to illustrate this, if we're talking about 6.1(f) disclosures, those are enclosures that the controller is entitled to but can't forced to be doing by the requestor. But we're trying to establish a system whereby ICANN can contractually enforce that data is disclosed under certain circumstances. So I think we need to get that terminology sorted as well.

Also, what we're conflating is what ICANN should govern and enforce and what is for the contracted party or ICANN to decide by itself. So there are numerous disclosure requests that are responded to today by registries and registrars, subject to national laws. And I think we should be very clear that if certain disclosure requests are not covered by our final report, that doesn't necessarily mean that disclosure is not possible.

But we're just talking about the small niche of things that ICANN should globally govern and enforce in terms of disclosure or access as the case may

be. And I think that we need to be pristine in our report to say exactly what we're doing and what we're not doing and, you know, I take the blame for not being more outspoken at this earlier, but I think that part of the issues that we're facing today is that we're not really clear on what we're trying to achieve here.

David Plumb: Thanks, Thomas. Okay, so Ruth, there's a lot of questions, some more specific than others, some very clear ones such as does ICANN need this purpose in order to have an access model, right? That I think you've heard two very different viewpoints in this room on. And there's other questions that have come up. Could you just take a moment for some initial reflections knowing that you may need to think about a little bit more, but what are some initial reflections on these issues?

Ruth Boardman: Sure. So I might just first come back and answer the first question which I think was from Benedict just before I forget it, which was if you have an organization who is requesting Whois data from one of the participants, then what are the rules that apply to that organization? And would they become subject to GDPR?

When you're looking at access to Whois data, you've got to look at it from the perspectives of the organization releasing the data and the organization requesting the data. So the organization releasing the data would have to be able to meet the requirements for a lawful basis under Article 6.1, as we discussed before most likely legitimate interests. The organization requesting the data would also have to have a lawful basis to obtain the data.

It might not be the same justification. As Thomas had mentioned, if you're a public authority, for example, then you wouldn't be able to rely on legitimate interests because the expectation is that the law that sets out your objectives will actually determine how you process personal data.

I'm also conscious that for law enforcement in particular there's an additional layer on top which is that for organizations in the EU the appropriate set of data protection laws for them are not GDPR but the directive which governs protection of personal data for law enforcement authorities. And one of the points that was mentioned in earlier advice given to ICANN was that there ought to be further work done on the interaction in that space. And I agree with that; I think - I'm not going to be able to give you the answer to that now but I think that that is something where it would be helpful to have further thought.

And you said, does accessing the data somehow make the organization subject to GDPR? GDPR has its own rules, as you'll be aware, as to when it applies and when it doesn't apply. So if you have - again if you take the law enforcement context, if you have an organization accessing data, Whois data, the fact it has come from another organization subject to GDPR does not necessarily mean that the recipient is subject to GDPR. If it's a law enforcement body in the EU then it will be subject to its own set of rules.

The exception to that where if you receive data from somebody, so registrar or registry, or others, to whom GDPR applies, the exception where receiving it will make you subject to GDPR is if when you access the data if you are asked to enter into standard contract clauses to govern the provision of the data, then through those clauses you agree to comply not with GDPR but with the set of principles which are based on the old directive.

So to give you a scenario, if an organization in the US or in - pick another country - South Africa or in India wants to access Whois data, if it is asked to sign up to standard contract clauses in order to govern the transfer of that data, then through those clauses and that organization would agree to comply with principles which are similar to GDPR, and in fact they're based on the directive that GDPR replaces. So maybe I'll stop there on that question. Okay.

I'm going to have a lot less to say I think on the other questions because the other questions really seem to boil down to how does - how does ICANN and all of the stakeholders in this room - how do you put in place a system where ICANN can enforce disclosure of information? So it's very easy to see or relatively easy to see from a data protection perspective how you justify disclosure if an organization wants to make the disclosure. So I think Thomas made the point that 6.1(f) permits disclosures but it doesn't mandate the organization to disclose.

The registrar or the registry or the other party is having to reach a decision itself as to whether or not it thinks that the disclosure is necessary and in the interests and that are covered by 6.1(f). If the question is, well how does ICANN put in place a structure that allows it to require other parties to disclose information, when it thinks they ought to, and what does it need to have in here to allow it to do that, that's a big question and I'm not going to be able to give a quick answer to that now off the top of my head.

David Plumb: So a fundamental question in the room, which was for ICANN to move forward with a standard access model, do you need to create this purpose, right, in order to allow it to move forward? And there's different opinions on that. You don't have an ability to answer that right now, Ruth?

Ruth Boardman: There are some occasions where I get answer is helpful and there are some occasions where you just need to think it through properly and this is one of those occasions.

David Plumb: I don't want to keep going; I want to take a break. All right, we're not going to keep going on this thread right now. And I think Kurt wanted to say a few things. We're going to take a break and then we're going to see where we are, all right, because I think we should all sort of chew on this for a second over break. Kurt, a few words to close us off before we head to our break?

Kurt Pritz: Right, I just wanted to make a comment about whether, you know, we need this purpose in our product in order to enable the creation of an access model. And I'm thinking about our progress and process as we march through this. And there are essentially four or so purposes in the temp spec that have to do with the disclosure of data or access to data and as part of our accommodations we got rid of three of them and collapsed them all into one. And then now we're discussing whether or not to eliminate that one.

And so our audience is going to see that there were four purposes having to do with the disclosure of data in the temp spec and this team potentially decided to eliminate them all. So what's that message that - to me that's a pretty clear message that we're not for the disclosure of data. And to me as part of - I'm talking, I'm talking. And so to me that's a clear message that says without anything else in our report that says that this team generally doesn't support this. And that's why I think it crests difficulties for ICANN to do it and it creates this perception that this group is not for that. And I think that's a fairly strong message.

David Plumb: I know folks would like to, you know, have a conversation with Kurt about that. So I think, why don't we take a break, all right. Let's stand up, get some air. We'll be back in 15 minutes, all right. And we're going to take stock and figure out what we're going to do about all this, so we'll take a 15-minute break and we'll be back.

END