ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Thursday, 07 May 2020 at 14:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/1iqJBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page:
http://gnso.icann.org/en/group-activities/calendar

TERRI AGNEW: Good morning, good afternoon, good evening, and welcome to the GNSO EPDP phase two team call taking place on the 7th of May 2020 at 14:00 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourselves now?

Hearing no one, we have listed apologies from Matthew Crossman of the RySG and he has formally assigned Beth Bacon as the alternate for this call and any remaining days of absence. All members and alternates will be promoted to panelists for today's call. Members and alternates replacing members, when using chat, please select all panelists and attendees in order for everyone to see the chat. Attendees will not have chat access, only view access to the chat.

Alternates not replacing a member are required to rename their lines by adding three Zs to the beginning of their name, and at the end in parentheses, their affiliation, dash, "alternate," which means they are automatically pushed to the end of the queue.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

To rename in Zoom, hover over your name and click “rename.” Alternates are not allowed to engage in the chat apart from private chats or use any other Zoom room functionality such as raising hand, agreeing or disagreeing.

As a reminder, the alternate assignment form must be formalized by way of the Google link. The link is available in all meeting invites towards the bottom.

Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now.

Seeing or hearing no one, if you do need assistance with your statements of interest, please e-mail the GNSO secretariat. All documentation and information can be found on the EPDP Wiki space.

Please remember to state your name before speaking. Recordings will be posted on the public Wiki space shortly after the end of the call. As a reminder those who take part in ICANN multi-stakeholder process are to comply with the expected standards of behavior.

Thank you, and with this, I'll turn it back over to our chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you very much, Terri, for introduction. Hello, everyone. Welcome to the 56th meeting of EPDP and usual question, are we prepared to follow agenda suggested by leadership of the team in the runup to the meeting?

So the agenda is displayed on the screen. I see no hands up. I take that agenda is adopted. So thank you very much. The housekeeping issues, so we have major development. As you saw in your mailbox, we received the SSAD model cost estimate and I will maybe ask Berry to talk a little bit about this document.

BERRY COBB: Really, nothing more than what was emailed out to the list earlier this week. Org did submit the discussion paper for the cost estimate for the SSAD. We will use next Tuesday's meeting, the 12th of May at the same time, 14:00 UTC. Xavier and his team will start off with a brief introduction to review the high-level aspects of the discussion paper, and then basically open it up for questions and general discussions about some of the findings in there.

The meeting itself is not mandatory, so it's really only for those that are interested in this particular topic. However, we would stress that it would be beneficial to have at least one person from each represented group in attendance so that you may convey back any of the high-level discussions or responding to questions that your particular group may have.

In particular, what will be helpful for the team that put this together is if you do have any advance questions or comments, please send those to the list and make sure to pass them to that team, and they can come prepared with some answers or responses to your comments as required. Thank you.

JANIS KARKLINS: Thank you, Berry, for this introduction. Any questions or comments at this stage? So from my side, I would like maybe to stress that the nature of the document is to inform our debate. We're not going to argue over presented numbers because they are only estimates based on our best guess on certain parameters of SSAD, but certainly, that gives us rather clear picture what we're heading at, so the question is for us to reflect what type of financial mechanism we should put in place in order to cover costs of the operations of the SSAD. And again, this document is informative and is just a reference for us.

So with this, I will move to the next sub-item on housekeeping issue, the comment period for initial report and addendum expired two days ago, so maybe we can have an update from the staff what's the status.

BERRY COBB: Thank you, Janis. As noted, both public comment proceedings have closed now. For the initial report, you'll recall that we extended it out to the same close date as the addendum report. We only received two comments back to the original public comment for the initial report. Those have all been incorporated into the PCRT tools as well as the discussion documents. You'll see on our Wiki page for the initial report that we're also using a color coding system to highlight which particular comments that the group has reviewed through. And as you can see, there's a few that are green and several that are still white.

Secondarily, in terms of the public comment on the addendum report, staff is working on the compilation for those. It will follow

the same process as the previous one. Just in general, we've had 21 total substantive submissions. There's still two groups outstanding. There were 12 organizations and two individuals. Just like last time, we did have a few submissions that were identical and we consolidated those into one master submission, but we still incorporated all of the organizations that have made that submission into that master. And then we also had three submissions that were incomplete.

So you'll notice on the same Wiki page, there's a section down below that will designate or delineate the addendum, particular comments. We're working on updating the PCRT tools. I should have those complete by the end of the day or tomorrow, but you'll be able to come here right away to start to be able to actually read the comments since the Google form isn't amenable to that. But it's still the same format. Basically, it's sectioned out by category of general support or not support for the recommendations. It has the actual comment that was submitted, who the contributor was, etc. and then of course, this information, just like what we're doing now, will be distilled down into discussion documents for the group to deliberate those, and here's your link, [Marc.]

That's all I have. Thank you.

JANIS KARKLINS: Thank you, Berry. Any questions to Berry in relation to public comment? I see none. Let me also use this opportunity to speak a little bit about the calendar. So if we do not count this meeting, then until the expiration or target date of 30 June, we have seven meetings. And certainly, seven meetings may not be enough to

review all the comments and suggestions on the remaining outstanding recommendations as well as do the final “cannot live” reading of the entire document. Therefore, I would like to seek your understanding and accepting that from, not week but week after, we reintroduce the second meeting on Tuesday of substantive nature and we work on Tuesdays and Thursdays hoping to review all comments and all recommendations, and the whole document in its entirety by 30 June.

So please be prepared. And I understand that fatigue has kicked in already and we see it from the way how comments come in and—but again, this is a final stretch and I plea your understanding and support that we can finalize our work by June 30.

So with this, I would like to go to the agenda item four, which is recommendation six. We started review of recommendation six last meeting. We went through first items, and I was told by staff that we missed one issue which is now outlined on the screen to provide additional guidance to ICANN Org, how to enforce necessary means, more desirable but less than indispensable or absolutely necessary.

So again, I recall that there was a long discussion about this issue in Los Angeles and I would like to see if proponents of this formulation could remind all of us what was the [essence.] Anyone? Mark?

MARK SVANCAREK: The reason that the wording is because there's always been debate about what data minimization means, and so the data has to be collected for a purpose, it has to be processed for that purpose, but you want to use as little data as possible and you only want to collect it and process it if it's necessary. So there's always been a debate about what necessary means. This is a definition that I think came from working party 29. I don't remember exactly, but it was quoted by Bird & Bird. This is the actual verbatim text from one of the opinions we got from Bird & Bird.

So it is here for clarification in case people wonder what necessary means, how that would apply to compliance. I guess that's an implementation issue. Now that somebody mentions it, it's like, hm, it could be interesting figuring out what that means. Thanks.

JANIS KARKLINS: Thank you. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I guess I was asking for the overall context. I guess while Mark was talking, I found it, and this was on page 26 of primary recommendation number six, contracted party authorizations sub-bullet point two, [inaudible] data elements request, request if necessary to the requestor's stated purpose.

So, and you said this is an ICANN Org question for clarification on contracted party authorization. Do I understand the overall context right?

JANIS KARKLINS: Yeah, this is what I was told.

MARC ANDERSON: Okay. Thanks.

JANIS KARKLINS: So most probably then the answer to ICANN Org request or question would be maybe it makes sense to review again Bird & Bird memo and see what—put it in the right context and implement that or figure it out during the implementation phase.

So in absence of further comments, I would invite now Caitlin to walk us through and introduce the next three points, I believe.

CAITLIN TUBERGEN: Thank you, Janis. And as Berry has highlighted on the screen, the next three questions correspond to the text, if the answer to any of the above questions is no, ... And this is of course the answer to any of the questions in the threshold test the contracted party is performing is no, the contracted party may deny the request.

But we've had some comments come through, the first two being about if the contracted party denies the request, should there be an ability for the requestor to appeal? Many agreed that they should be able to appeal but the question is how should that appeal look and who would be the arbiter. And I would note that here contracted parties provided comments that the arbiter should be the DPA.

And then similar to question six, question seven is also asking if before the contracted party denies the request, should requestors have the opportunity to provide further information before the official denial? So in other words, should there be some sort of intermediate step before official denial?

And then last, we had a question from ICANN Org regarding if any sort of implementation guidance could be provided in relation to questions such as must contracted parties go back to central gateway to request more information, or would alternatively the contracted party interact directly with the requestor, and how that type of interaction should take place. And I'll note that the EPDP team members who responded to this question in the discussion table noted that high-level implementation guidance should be provided but there were no examples actually provided in the response. So here we're looking for guidance on what that implementation guidance should be.

JANIS KARKLINS: Thank you, Caitlin. Stephanie, your hand is up. I assume that this is on the previous issue.

STEPHANIE PERRIN: Yes. I just wanted to note here that I'm a little confused as to what we are handing over in the way of determination of data minimization to the IRT. Generally speaking, general guidance on data minimization would not be handed off to the IRT. We need some goal posts and we need to determine whose accountability it is to make that decision about what data shall be released given a

certain type of request. And as far as I'm concerned, that discretion on the release of the data rests in the hands of the contracted parties, period.

Since we're already on this next issue, which I think I've pointed out before and I'll do it again, there is no way that the data protection authorities are going to be a referral mechanism for disagreements between the requestors of data of registrants. That is not their role. I haven't reviewed all of the different legislation but I'm pretty sure they're not authorized to do it, and they are busy enough. Thank you.

JANIS KARKLINS: Thank you, Stephanie. So you covered both—I think that this is understood that those who make disclosure determination or decision will be the ones who will determine how much information should be handed over to requestor, because that is also their liability.

So let me now move to the questions about whether there should be appeal mechanism and how this appeal mechanism would look like. Margie, your hand is up followed by Mark SV.

MARGIE MILAM: Hi. Thank you. I was going to say a lot of what Stephanie was saying in regards to it's just not the role of DPAs to get in the middle of a decision like this. So I would reiterate the request that there should be some sort of appeal mechanism for wrongful denials. So I think that's something that we should build into our

policy given that the DPA is not going to be one that is going to be able to address these issues.

JANIS KARKLINS: Do you have any reasonable mechanism in mind how that could be organized?

MARGIE MILAM: We have examples. I think we mentioned this before in other cases in GNSO policy. So you could look at the new gTLD program, you could even look at the UDRP. You make a request, there's a couple panelists selected to review it, and it's not likely to be abused if there's a cost associated with it for the requestor.

So I don't think it's unreasonable to expect that ICANN would create some sort of lightweight mechanism similar to what already exists.

JANIS KARKLINS: Okay. Thank you for proposal. Mark SV followed by Volker.

MARK SVANCAREK: Thanks. Stephanie made a point about who is the decider in the hybrid model, it's the contracted party. I don't have any objection to that, but it does go to the whole reason why that definition of necessary is in the policy, because we do want to make sure that during the implementation phase, everybody has as common understanding of what can be disclosed.

We've had a lot of historical discussions about this topic, and if we go into the IRT without this definition, without this statement in there, we're just going to have to relitigate those conversations again. So although I agree with her statement, I don't think it changes the fact that this language should remain in this policy recommendation. Thank you.

JANIS KARKLINS: Thank you. Volker, please, followed by Beth.

VOLKER GREIMANN: I understand the desire to have some form of appeals mechanism like the UDRP or something like that, just in case something doesn't work out the way that we've planned it or that we're foreseeing it. However, I have a bit of a stomach ache on the topic of who will be able to tell a contracted party that they have to disclose a certain set of data when the contracted party has already made a determination that they are not legally able to do so.

Putting a third-party panel in there that might not have the same expertise or based on the same jurisdiction, it certainly cannot be compliance. It's just asking for trouble. Basically, we're handing over control of releasing date through this party. And before we can agree to do that, there would have to be very significant assurances that this will not be abused either, and this panel or whatever it is will have the necessary expertise and knowledge in our respective jurisdictions to make that determination based on the facts that are available. Thank you.

JANIS KARKLINS: Thank you, Volker. And what would happen if panel would overrule the decision of contracted party and then that decision would be challenged by data subject for instance? And data subject would be right. Who would be held liable for release of data? And who would pay the fine? Just a reflection question. Beth, please, followed by Brian.

BETH BACON: Thanks, Janis. You and Volker kind of stole my thunder there. I would like to put a little finer point. While I understand there's a desire to say, well, I'd like a second opinion, the second opinion would have to be—as a controller, if you read the GDPR and the way the language is phrased, we have to make the decision based on our analysis. If you disagree with the analysis, you could say that to us and we could relook at it again. However, anything beyond that doesn't really exist, simply for the reason that Janis just pointed out. Where would that liability live?

If we went to a panel of folks and they said we disagree, you have to release this person's data, I don't see a controller on this call or in this environment being comfortable saying, okay, sure, I will now release that private data because you told me to, and override the analysis [inaudible]. I think it's a very squishy prospect, and it would be very concerning, I think, for anyone who had to try and implement that.

JANIS KARKLINS: Thank you, Beth. Brian, followed by Stephanie.

BRIAN KING: Thanks Janis. I hear a lot of the concerns that have been raised. I think there have been a lot of good points raised here. I think the challenge for us is that not all contracted parties will be subject to GDPR. Certainly not all registrants are. However, the policy in order to be universally applicable is going to give the ability to all contracted parties, whether the law warrants it or not, to deny these requests. And our experience has indicated that many contracted parties, if they're able to ignore, deny or otherwise kind of just paper the file but not provide the data anyway, will do that, whether the law applies or not.

And I think that while I am sympathetic to the concerns that have been raised here, in many cases, the law simply won't justify the decision that's been made and we need I thin Kerry Ann way to appeal that, at least in those limited cases anyway. So probably worth thinking about that more.

JANIS KARKLINS: Thank you, Brian. Stephanie, please.

STEPHANIE PERRIN: Thank you. I think this is indeed a difficult problem, and let the record show that I actually have quite a bit of sympathy for the intellectual property and business folks because not all registrars are going to comply.

So hence my interest in data trusts and some kind of advisory panel or board with multi-stakeholder representation that would

hear these cases, dismiss the spurious ones, and act on the what I would call bad actors. I do not actually think that GDD can take this on, they don't have experience in data protection law. I think it may bias their other activities. It's not really germane.

However, it could have results of disqualification of registrars as being accredited, because failure to comply with law and policy is certainly part of the accreditation requirements and will remain so, I would think.

So that's the mechanism that I would recommend. The problem, of course, is that if you set up such a mechanism, you cannot leave the liability resting with the registrars and registries. The liability passes to ICANN as co-controller in establishing such a mechanism, probably through a processing arrangement because of course, you will be processing data in order to evaluate the requests.

That's my two bits on how you could do this, and I do think that if the mechanism was properly constructed, if it was multi-stakeholder, if it was well versed in data protection law which ICANN is, with all due respect to those present, not really, it's not really their bag, nor should they make it their bag, then I think that a court or a DPA would view that favorably and not be likely—because you've done your best and there is a legitimate counterbalancing argument here in the release of data. So I think that's the only way to do it. But ICANN's got to bite the bullet and take on that liability. Thanks.

JANIS KARKLINS: Thank you, Stephanie. Wouldn't that be something feasible to introduce kind of ombudsman-like process where in ICANN—I believe that there will be a privacy officer or something like that who could then be also acting as ombuds in case of disagreement and certain disclosures and could also supervise from ICANN's side functioning of SSAD in general.

Margie.

MARGIE MILAM: Hi. Thank you, Stephanie. I actually think what you proposed is along the lines of what might address our concerns. I don't care what you call it, reconsideration, whether it's some sort of advisory panel, and pretty much giving it an ability to address situations that are just flat our erroneous, and then that sort of information could always feed into a compliance thing later on at ICANN if the particular contracted party just continuously decides not to disclose and has a record of simply not disclosing and then panels found against them. Something to that effect. So I really do think that that's probably something that would help and would make sure that the decisions are made by people who are knowledgeable about the data protection law and that there's some sort of oversight. Thank you.

JANIS KARKLINS: Thank you, Margie. Mark SV.

MARK SVANCAREK: Thank you. I just want to remind everybody that we are planning to build a secure logging system as part of the SSAD, and this is one of the reasons for it. If there is a requestor who has unexpectedly high rates of bad requests or rejected requests—bad being they're ill formed when they're submitted, and rejected just means rejected, and if there is a controller that has unexpectedly high rate of rejecting things that are judged to be well formed, then that's data that would be available to whatever his mechanism is to determine if somebody is systemically an offender, as Milton suggests.

So as long as we've got the accounting available, the objective measuring, then we can move ahead. And of course, if you are a systemic offending requestor, you'll get deaccredited. We don't have a similar concept for systemic rejectors, people who are just rejecting out of hand or automagically or whatever. But that's an issue for us to deal with in a different section, I guess. Thank you.

JANIS KARKLINS: Thank you, Mark. I think that Margie was talking about appeal for individual disclosure rejection. You're talking more about systemic issue.

MARK SVANCAREK: What I'm saying is if you are evaluating whether a particular thing should be appealed, the past history of the parties could play a role in that, and that's what I'm mentioning.

JANIS KARKLINS: Okay. Thanks. Thomas.

THOMAS RICKERT: Thanks very much, Janis. I've put this in the chat already, but [inaudible] the original proposal has sort of [inaudible] I put my hand up.

I think what we're really discussing is not an appeals mechanism but a request for reconsideration mechanism to give the contracted parties the opportunity to be reminded that the contracted parties might not have taken all of the facts [it had] into consideration and based its balancing test where applicable on that.

So maybe a way forward could be to make this a reconsideration request. Then I think even though Milton is already complaining that we're making this too complicated, I think it is actually complicated, because we have to look at what the legal basis for the disclosure would be. If there is a requirement for the contracted party to disclose, then I think the original requestor who has a legal right on the data potentially needs to go outside of the SSAD and try to force that claim directly with the contracted party. But the vast majority of scenarios will be disclosures based on 6.1(f) where the requestor does not have a right to the data but the contracted party has a right to disclose if they think the balancing test is in favor of disclosing the data.

And therefore, I guess the question is how can you force somebody to do something that they are entitled but not legally

obliged to do? And that's, I think, where the contractual framework for the SSAD needs to be good and solid.

We need to have contractual language for contracted parties with the SSAD whereby contracted parties that systemically try to not disclose data because they either don't apply a balancing test or the balancing test is plain wrong, then ICANN Compliance needs to be able to sanction that. But where there is a fine line between being able and not being able to disclose and where the discretion is exercised in an appropriate fashion by the contracted party, the ultimate disclosure decision needs to rest with the contracted party.

JANIS KARKLINS: Okay. Thank you, Thomas. Can we then gather around the idea that requestor may ask reconsideration by the contracted party? At one point, we need to move on, so I have now many hands up. Volker, Alan G, and Milton.

VOLKER GREIMANN: Thank you. Janis, your suggestion is not a bad one. I think a reconsideration request can be possible where it's directed towards the contracted party that made the original decision I the requestor feels that something was not taken into account or some additional evidence has emerged. But that shouldn't be taken against our SLAs. We have provided the answers so the SLA is done for that request.

There is another reconsideration request that maybe people are not seeing so well, and that's the courts. If you have a legal right

to access that data, the SSAD is mainly a shortcut. You still have the right to go to court and to request disclosure of that data through a warrant or a subpoena or any other legal mechanism that's available in the country, where the contracted party is at.

And you will even be able to prove that you've already made a request to that party and might even have certain cost elements in your favor if you choose to go that route, because by denying that request in the first place, they might have shown bad faith depending on the legal system you're operating in, that might be a cause of action. So the courts are always available. Thank you.

JANIS KARKLINS: Thank you, Volker. Alan G.

ALAN GREENBERG: Thank you. The courts are certainly available, assuming there are courts that would hear it in a timely manner at a reasonable cost in the jurisdiction where the contracted party resides. And that adds a whole bunch of potential problems in using that process.

the logical conclusion to me of what Thomas said is since the decision rests on the contracted party and they are not obliged under GDPR type law to release information, then it must go down to the contract requiring them to release information unless they can demonstrate or otherwise show that the law prohibits it.

So it really has to come down to a contractual clause that they are obliged to do this unless they have some overriding reason and have to be able to explain what that is.

I don't see any other way of getting around this. Thank you.

JANIS KARKLINS: Thank you. Milton.

MILTON MUELLER: Yes. I feel like we're kind of losing a sense of proportion here, a sense of the overall context in which these decisions are going to be made. So yes, it's possible that some registrars will not be responsive. They may routinely reject everything, they may routinely accept every disclosure request. There's all kinds of ways in which at the discrete level, things can go wrong. But let's keep in mind that there are going to be—I don't know, hundreds per day of these requests, thousands, maybe millions in the course of a month. We don't really know, but based on the way some people used WHOIS in the past, we can expect there to be a very high scale.

So the idea that every single discrete disclosure decision is going to be subject to a complicated appeals or reconsideration process strikes me as bizarre, as we have completely lost sight of the overall context of this.

Yes, there should be mechanisms by which abusive registrars in either direction could be sanctioned or reaccredited just as we have set something in motion for people who request in an abusive manner, but when you start talking about appeals of every single discrete decision, I think that's just prima facie absurd and we just can't do that. This is not that kind of a system. This is not a judicial determination of disclosure, this is a semi-automated

system of getting information efficiently and rapidly to people who have a legitimate interest in it.

So any kinds of appeals or sanctions have to be at a much higher level of the process at the level of consistent behavior being challenged by ICANN Compliance or something like that. And if you're going to have this appeals and reconsideration process for the requestor, then you've got to have it for the registrants, for the data subject as well.

So let's not get so burrowed down into the details of this process that we lose sight of the overall context. Let's come up with some generalized sanctions or accountability mechanisms and leave it at that. Thank you.

JANIS KARKLINS: Thank you, Milton. Margie.

MARGIE MILAM: I think the problem we have is that we've got accountability on one side, on the requestor side, but not on the other side, and that's really what we're talking about here. And I just don't see Milton's concern about this being abused, especially if there's some sort of cost associated with filing the reconsideration. You don't see a lot of UDRPs for the same reason, because the costs associated with filing UDRPs. So if there's going to be a challenge, it'll be because the requestor believes that they have a legitimate reason to ask for reconsideration.

And I don't agree that the reconsideration only goes to back to the contracted party, because if the contracted party has decided just as a matter of course that they are going to say no to every single request, a reconsideration isn't going to change that.

So the concept that Stephanie was talking about, which is the concept that I support, is some sort of third-party advisory panel or a panel of experts that can weigh in on what's reasonable in the situation. And that's the only thing, I think, that would really work.

JANIS KARKLINS: Thank you, Margie. So wen it comes to systemic analysis of the work of SSAD, we had the proposal in recommendation 19 on evolutionary mechanism, and there's one of the topics this mechanism would look at is operational efficiency of SSAD based on data which will be collected in a systematic way. and if there is an obvious systemic issue, these issues will be addressed in one way or another, or at least indicated.

So maybe we could think that this mechanism takes care of the systemic issues that Margie is referring to. Amr.

AMR ELSADR: Thanks, Janis. I agree completely with what you just said. If we're looking at systemic issues like the ones that Margie just described, of a registrar or a number of registrars that are just rejecting all disclosure requests, then a process similar to the one that Milton suggested should be able to flag that and then hopefully fix it.

But I think another reason—and just to add to what Milton said earlier, another reason why a higher level of an appeal would be more suitable on a case by case basis is that we don't want to slow down the process of disclosure requests. Even in the case where disclosures are granted, if we have an appeals mechanism on a case by case basis, in cases where disclosure requests are rejected, and we similarly need ones for ones that are approved, then the registration data won't be disclosed as soon as a decision is made. There would have to be some sort of notification to the registrant that there's been a request to disclose your registration data, you have for example like five business days to appeal this decision. And that would ultimately slow the process down.

So I think there is merit to exploring a higher level of appeals that address systemic issues rather than on a case by case basis. Thank you.

JANIS KARKLINS: Thank you, Amr. Beth.

BETH BACON: Thanks very much. I wanted to address quickly two things. One, I'm supportive of thinking of a way for folks to come back [to a contracted party] and say, hey, I think I disagree with your balancing test. Because it is a human review as required, and humans are sometimes wrong.

So I don't have any problem with that. And certainly, keeping systemic abuse in check is very important in any process. So of course, don't object to that. I do however have concerns—Margie

noted if a contracted party decide they're just going to say no to every request, in that case, they're neither following the law nor are they following consensus policies.

In phase one, we already have a requirement to provide a balancing test when appropriate or when required. So if a contracted party is not following the law and not providing the balancing test when they're supposed to and they're just rejecting, then you don't need a reconsideration request. You need Compliance. Because they're not following their contractual provisions via a consensus policy.

So I do think, along the lines of what I think Amr was saying, we need to make sure that we are narrowly the solving the problem that we actually have as opposed to using every issue to solve every problem, which is to bring something to Compliance. Because that's not always the solution. In that particular one, I think it probably is, because they would be not following their contract. However, I do think a reconsideration of certain—either one offs if you disagree or a systemic issue. I think those are actual issues and we should have a solution for those. Thanks.

JANIS KARKLINS: Thank you. And Laureen, you have the last word.

LAUREEN KAPIN: Good, I love having the last word. I actually agree with many of the comments expressed, and though they may seem to be inconsistent, I don't think they really are. Milton has a good point about not making this too complicated, and skepticism expressed

about creating complicated systems, I think, is well taken. At the same time, we do need an efficient mechanism, something that is quick, and to me, that doesn't fall into necessarily recommendation 19 or even ICANN Compliance. I think we do need some sort of separate lane to deal with both systemic issues quickly and the occasional one-off that may occur where you want just a quick second look. And I think we are very capable of coming up with something that might be able to deal with both those situations.

JANIS KARKLINS: Thank you, Laureen. I said that this would be the last word, and Hadia, if you wouldn't mind to take your hand down. I got a message from staff that they have enough material to write up a proposal in the final edition of this recommendation, so encompassing everything that had been said, and then views expressed in this conversation, thinking about efficient and not really complicated mechanism that could allow all parties, requestors and then contracted party to communicate quickly and resolve issue if there is one. And then of course, there are systemic issues that will be reviewed by the evolutionary mechanism that we will review in one of the next meetings.

Thank you very much. Now the next question is about how the information exchange or communication should go either through central gateway in case of necessity for additional information or directly between contracted party and requestor. Any guidance? The question is now outlined on the screen. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I think this is a really important question for us to consider, and I'm not sure I've worked out an answer on this one that I can recommend. But I think it's important that we determine how a requestor who goes to the central gateway [inaudible] central gateway is going to communicate with the contracted party that they're expecting disclosure from, whether this be request for additional information or how the information would be delivered back to the requestor, which is required to be done in a secure manner, whether that be passed through the central gateway which creates liability issues with the central gateway itself, or whether we're creating a separate mechanism for the contracted party to respond back to the requestor.

So I think this is an important question we have to spend as little time on, make sure we have a common understanding and provide clear guidance to the implementers. As has been mentioned today, if we don't provide guidance on this, this is going to seriously bog down the IRT. So I suggest we spend a little bit of time on this and make sure we think this through.

JANIS KARKLINS: Okay. Thank you, Marc. James.

JAMES BLADEL: Thanks. Just echoing Marc, I think that this is perhaps a pitfall that we've overlooked. I'm not claiming to be an expert on this particular aspect of the law, but I don't think that we can just casually fire off any sort of disclosure information in an e-mail

back to a requestor. That certainly wouldn't fly. I think we should consider whether there is an in-band response where the SSAD relays a response from a community to the requestor in some sort of secure fashion, or whether there's an out-of-band response where it's happening outside the SSAD. And I think either of those probably could work so long as that they were encrypted and secured in some way that it wasn't just sending personal information in the clear.

I think we need to figure this out, and I think we need to consider both the operational time to develop something like this, because there are going to be complexities, there are possibilities that things might not work at scale, and that could introduce delays in implementation, not to mention an whole bunch of costs for SSAD and contracted parties. But setting that aside, I think we want the thing to work and we want data to be handed back and forth in a legal way.

So I think we do need to spend some time on this. It is one of those things that is not the sexiest part of what we're talking about here, but it is important. Thanks.

JANIS KARKLINS: Thank you. I think there's a bit of a confusion. The initial report suggests that this disclosed data should be sent from contracted party directly to requestor in a secure manner. But the communication should be from contracted party to requestor.

Here, question is if you need additional information to make this determination. And since the request comes through the central

gateway. So the question is if contracted party needs additional information, this additional information requested by contracted party from requestor is sent through the central gateway or directly, the communication is directly. It's not about personal data, it's about request for additional information or clarification questions that are needed in order to make disclosure determination. So that should be rather simple.

Hadia, what do you think?

HADIA ELMINIAWI: Thank you, Janis. When the central gateway actually receives the requests from the requestor and decides to pass it to the contracted party, it certainly opens a ticket for that. And then forwards it to the contracted party. So it does make sense that if the contracted party needs further information, that it goes through the central gateway for that information.

I think what James was talking about—so what if that additional information that is going to be relayed to the contracted party includes some kind of personal information? And the solution for that is of course some kind of encryption so that the central gateway doesn't necessarily need to see what's relayed from the requestor to the contracted party. But nevertheless, the answer goes through the central gateway.

So my answer to that question would be that, yes, the central gateway would open a ticket with the requestor and that any additional information required by the contracted party should be relayed through the central gateway. And in case the information

relayed from the requestor to the—it should not include any kind of personal information, because it's from the requestor. But nevertheless, if there is something that the central gateway shouldn't see—and I don't really envision this happening, but just in case there is some kind of information that the central gateway doesn't need to see, it could be encrypted.

But in all cases, the requestor in the first place when he submits the data to the central gateway, he submits all the data and the central gateway reviews the data. So that shouldn't be any kind of request requested from the contracted parties to the—request shouldn't be different than any kind of data that would have been originally given from the requestor to the contracted party.

So in short, yes, it could be relayed through the central gateway.

JANIS KARKLINS: Okay. Thank you. Volker, are you in agreement with Hadia?

VOLKER GREIMANN: Yes, surprisingly. I think that's probably the best way forward. And I also think that we should have this feedback loop that while going through the central gateway for trackability and evidencing of the communication that has gone on, maybe not the contents but that there had been communication between the parties, I think it should go through the central system, and encryption is probably the way forward here.

I also think that this feedback loop should be there. It is currently there in the status quo and we're looking at improving the status

quo, not making things worse than they are, so we should have the ability of the contracted party to request further information in case that just a little bit is missing before they can make a positive decision, for example, instead of having to refuse it and forcing the requestor to do another one. So having that in place is probably the right way.

And finally, for the question that was briefly touched upon of the data disclosure, the way that I have envisioned the central gateway to work was always that it would probably make an RDAP call with a certain password and that would unlock the data at the contracted party in their RDAP server so the central gateway would make that a request and pass on the data in an encrypted format to the requestor.

So depending on how we build this technically, this will probably make the most sense. Thank you.

JANIS KARKLINS: Thank you, Volker. So we seem to be converging that communication should go through the central gateway. Brian.

BRIAN KING: Thanks, Janis. I think I agree with what everyone has said, including your last synopsis, and I don't know that I would add more besides to say that we are getting a little technical for perhaps what we've been asked to do here. And if we're in agreement, let's take that agreement and move on. Thanks.

JANIS KARKLINS: Thank you. Marc, you're in agreement, right? Marc took his hand down. Then it'll be probably provided in implementation guidance that the communication between contracted party and requestor should go through the central gateway when it comes to request for additional information.

Shall we now move to the next one? Point nine. Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. Question nine deals with the text about where disclosure cannot be used solely for certain categories. And the question nine is in reference specifically to the text following the second semicolon where it says nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement.

So there were some issues with that text. Some commenters noted that it should be stricken entirely and other commenters say that retention of that text is important. So we're looking at a way forward here and how the concerns could be addressed.

I think some of the contracted parties [who've commented have] noted that that text may limit their discretion and deals with content that should not be addressed by the registrar or the registry.

We were thinking that perhaps it might be that we could add a footnote here that it's not saying that contracted parties are not entitled to deny a request, but they cannot solely deny a request based on this. But we're looking for further feedback here. Thank you.

JANIS KARKLINS: Okay. I wouldn't like to repeat the hours of conversation on this topic we had in Los Angeles. Milton, please.

MILTON MUELLER: Thank you, Janis. I wasn't in Los Angeles so I am completely liberated from any worries about repeating a conversation there, but I just don't understand why it's in there. Nothing in the policy says that intellectual property infringement is not a legitimate interest. In fact, I think there was a couple of things in there that specifically said that it was. And are there any instances of registrars specifically saying, hey, this is intellectual property infringement request, we're going to deny it simply because of that? Why do people feel like they need this, and do we want that kind of special pleading, this particular singling out of particular kinds of interests in the policy? I think we don't. I think that it's implicit, and sometimes explicit, in everything else in the policy that IP infringement is a legitimate interest for particularly trademark for domain names. So what's the problem here?

JANIS KARKLINS: Problem, Milton, is based on current situation where many of requests are rejected because they are of that nature. And we discussed it hours in Los Angeles. Brian, you can confirm that, right?

BRIAN KING: Thanks, Janis. I can confirm that that is a common reason for denial of requests. And yeah, not to rehash what we talked about in LA. I would just add constructively since it has been some time that this language was stolen verbatim from the PPSAI, which has a strong correlation to what we're talking about here. So this is an important one for us. Thanks.

JANIS KARKLINS: Thank you. Alan G.

ALAN GREENBERG: Thank you. I guess given that we have been told that it is a common reason for refusal, and the sentence does include the word "cannot refuse it solely based on it being intellectual property issue," what is the objection? I understand it would be better not to have this level of detail in a policy, but if we know it's an existing problem, then what's the harm in putting it in? Thank you.

JANIS KARKLINS: Thank you, Alan. I would like to suggest that we keep the text as is, but I have additional hands up. Stephanie and Alan Woods.

STEPHANIE PERRIN: I was in Los Angeles and I have painful memories of this getting in. I can't remember what I said in Los Angeles, but I think that the argument for taking it out is that we are singling out one particular species of request and justification for the request, and there are plenty of others that could also be discriminated against.

And for instance, it could be the Egyptian law enforcement which some might feel is a valid reason for refusing the request, particularly if you're related to one of the 60,000 people in jail. But that doesn't make it right. So pulling this out as if it were one particular of the many examples. That kind of guidance belongs in the implementation area, and I would punt this one to the IRT. It can't belong in the policy, it just can't. You could have a more general statement in a policy saying you cannot deny a request simply because it belongs to a particular category or type. You can do that. But to pull out one specific example because it happens to be well represented at ICANN, I think is not correct. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Alan Woods.

ALAN WOODS: Thank you. Again, also I was honestly in Los Angeles as well and I find it difficult to recall, because I remember specifically having this conversation in that and me specifically stating that this was, as it's written here, it is a limitation on the registrar and the registry. And I think Stephanie made a very good point there and that is you are specifically singling out and giving a special dispensation to one particular group over every other one.

And as I said in LA—and I must go back and review the transcripts I think personally myself because I don't know where it went at this point, is that is a perfectly valid reason to deny a claim. In fact I got two today, this very morning, which said the

reason for disclosure was being requested was “because I have a trademark.” Not because I need to do X with that data, not because I'm following this or that, but my reason is because I have a trademark. That to me is a perfectly okay reason to say no, to go back to them and say that is not enough, that is not a purpose, and I do not think we should be cutting our nose off to spite the face on this one. We should not be prevented by a policy to actually doing our job as a controller. And in this particular instance, this would be a disservice to anybody trying to make an actual claim, because you would have to go against ICANN policy in order to follow the law, and that is one of those things that we would want to try and avoid, I would assume, in such matters.

So I do have an issue with this. I think that we can put in additional safeguards that might appease the BC and the IPC in this instance, but the way it is currently written is far too broad stroke.

JANIS KARKLINS: Okay. Margie.

MARGIE MILAM: Hi. I remember the discussion in Los Angeles. This is really important to the BC. It’s part of the current consensus policy for the PPSAI, and it essentially, I don’t think, Limits what Alan is talking about because it says refuse solely for the lack of any of the following. So even in Alan’s example, if the only thing that is cited is that it is a trademark and there's no allegation of infringement, this wouldn’t even apply.

And the purpose of the SSAD is to allow disclosure in areas outside of the legal process. That is the fundamental reason why SSAD is even there. So I think this is basically clarifying why we have an SSAD, that we're not going to limit disclosures to only court orders or subpoenas or pending civil litigation, and this is consistent with prior GNSO policy. So we would object to taking it out.

JANIS KARKLINS: Thank you. Mark SV.

MARK SVANCAREK: Thank you. I think the example that Alan raised is a different problem. It's a malformed request. I think we have safeguards elsewhere in the policy where you would have to say what processing you're doing and for what purpose you're doing and by that standard, the requests that he received today would not meet—they're not well formed. So that would not be an example of rejection just because it's an IP request. It's a rejection because the requests themselves don't meet the requirements of the policy. So I still support this language and I just want to clarify that. Thank you.

JANIS KARKLINS: Thank you. Stephanie.

STEPHANIE PERRIN: This is a follow up on Margie's comment. I think that gets actually to the heart of what drives me nuts about this particular piece. If the SSAD is a shortcut to avoid legal process, and you're going to tell the affected parties that they may not say "use the legal process to get this data, I am not going to evaluate your request and make a decision myself," then you should say that.

What we're saying here is we're singling out vaguely one request. And what is essentially a legal matter. And if the SSAD has been set up to avoid legal process, then it should say so. And I think that's the heart of the matter and that's what we should have come out of the Los Angeles arguments with, language that reflects that we're shortcutting the legal process and that ICANN as co-controller is going to accept accountability for that. thank you.

JANIS KARKLINS: Thank you. But this is at the beginning of this recommendation. Absent of any legal requirement to the contrary. So that already suggests, in my understanding of this sentence, that we're talking about that there's no neither court order nor subpoena. So we're back in that conversation that we had already once, and of course, it was not a clear cut sort of decision, it was part of the compromise that we reached in Los Angeles. And now by just discussing this, we're kind of undermining our work that we did already there. Milton, please.

MILTON MUELLER: Yes. A very simple and constructive proposal to resolve this controversy, and I'm sure as soon as I propose it, everybody will nod their heads and we'll be done.

So it is in the chat. All we have to do is balance approval—or refusal. So instead of just saying nor can refusal to disclose be based solely on blah-blah, we say nor can approval or refusal to disclose, and that would, I think, at least handle, absolve some people's objections to the language and we could move on.

JANIS KARKLINS: Thank you. Basically, you suggest that nor can approval or refusal be—and so on. So if that is the price to pay, I would suggest that we do it. Hadia.

HADIA ELMINIAWI: Okay, so first off, I do agree with Milton's proposal. And just to Stephanie's point, the SSAD was never a short path to avoid a legal process. It is a path to protect registrants and the safety of the people online and the Internet ecosystem. And as Janis said, the recommendation starts with "absent any legal requirements."

Also, just a quick comment on what she previously said, I don't get how 50,000 or whatever the number is of prisoners in jail has any relevance to intellectual property infringement, and I'll stop here. Thank you.

JANIS KARKLINS: Thank you, Hadia. So then we have a solution, Margie, right?

MARGIE MILAM: I'm sorry, no, I don't agree with this, because what you're really saying here is that the contracted parties have to make a judgment on whether an IP infringement is valid, and that is simply not the case. That is not what contracted parties are here to do, that is not what the SSAD is meant to create.

Now, if it's something that—I don't mind something that's like good faith or something like that, but to have a contracted party make a determination on whether someone actually has infringement is really a problem, and that's why this language doesn't work for me.

JANIS KARKLINS: No, this says that the disclosure cannot be denied only because it is intellectual property infringement. And what Milton has suggested, that disclosure cannot be either granted or denied solely based on that fact.

MARGIE MILAM: I guess my question is why not? What is wrong if it's an alleged IP infringement and—think about this. The accreditor is accredited, they've already provided proof of their trademark, the domain name includes the trademark that's reflected in the registration. Why isn't that sufficient? I guess that's really my question.

JANIS KARKLINS: Okay. Brian.

BRIAN KING: Thanks, Janis. I don't think we like this either, especially if this is going to preclude automation. And what the language that has been proposed here also does is generalizes this way too much into founded on alleged IP infringement.

So what we had to kind of balance that was kind of struck in the previous language is that it was limited to website content and that it couldn't be rejected just based on the fact that it was website content and not a trademark in the domain name. That's an important point too, and flipping it and removing that does not just make it equal. That really skews the balance.

So what we're looking for here—and I can't emphasize enough the importance of the word "solely" here. If the complaint is lacking for any basis or if the contracted party thinks that IP weighs so low in the balancing test that almost every case would come out in favor of the data subject, this wouldn't even apply. We have solely here, so all this does is say that you can't reject requests just because they relate to IP on the website. And if you want to be able to reject requests just because they relate to content on the website, then we have a big problem with that. So I don't understand the hesitation about this language. Thanks.

JANIS KARKLINS: I think what was suggested by Milton is on the screen. So "solely" is not touched. Nothing is changed, only "or approval" is added in the text. This is what Milton suggested, and that is price to pay to get past on this disagreement.

BRIAN KING: Thanks for clarifying, Janis. I think that's not going to be acceptable because that removes what we think is a real opportunity for contracted parties to automate these if they feel comfortable. And that is something that we're not going to be able to live without either.

JANIS KARKLINS: Honestly, I do not see any connection with automation.

BRIAN KING: I can tell you, maybe elaborate a bit more on where we're coming from. We wouldn't agree that approval of the request be based solely on the fact that the request is about IP on a website. Many contracted parties may want to automate that request and have it be based on the fact that there's IP infringement on the website.

JANIS KARKLINS: No, I see that you have—and you need to follow the same process in approving or refusing. And you cannot neither approve nor refuse if the sole reason is that this is alleged IP infringement, full stop. Nothing else. I really don't understand the problem that you see with this one if that is something we could approve and get over. Anyway, Milton, please.

MILTON MUELLER: I appreciate your comments, Janis, because we're all kind of probably a little bit puzzled now. It seems that Brian and Margie

are basically talking us out of ever wanting to approve the original language without my modification, because what they're saying in effect is that they really do want automated approval of disclosure based solely on an allegation that there's an intellectual property infringement. And all we're trying to do is say, yes, it is incorrect for a contracted party to refuse to disclose based on the fact that it's an intellectual property infringement, an alleged one.

That is not just, but it is also not just for them to automatically approve it simply because you have alleged intellectual property infringement. Indeed, if you know the history of ICANN, this is how the whole UDRP got started, was because Verisign was simply looking for a string match with trademarks and all you had to do was assert a trademark over a string and they would take down a domain even if that domain was something like Miller and your last name was Miller, because there was a trademark on Miller. It was manifestly unjust, and we're just trying to balance this and we're conceding to you that nobody should refuse to disclose based entirely on the fact that it's an intellectual property allegation, but by the same token, nobody should approve that.

And if you can't accept that, I think that you are giving the rest of us absolutely no reason to respect your concerns about the original language. Thank you.

JANIS KARKLINS: Thank you, Milton. Mark SV, please.

MARK SVANCAREK: Thanks. I guess my intervention is—the world has passed on beyond it. I just want to remind everybody that some of the examples that are being put up, reasons why to accept language or not accept language, are based on the idea that the requests are inherently bad. As I said before, misformed requests, incomplete, stuff like that. So just when you're considering this language, assume that these are good requests, that everything that we require in the policy is in them, and that this comes down to just this one aspect of the request, whether it's related to IP or not. Thanks.

JANIS KARKLINS: Thank you. Brian, please.

BRIAN KING: Thanks, Janis. I'm taking Milton's point, and I do want to be reasonable here. I want to invite everybody to come to agreement. So I'm wrapping my head around the "or approval" language. I'm thinking worst case scenario though in this, the "or approval" I think does perhaps give us some heartburn about the fact that this might preclude automation or how—I'm just thinking about how it could be misconstrued. I don't want this misconstrued to prevent automation of these cases, nor do I want this to be misconstrued to say that any requests based on IP content—that the entire request—I guess what I'm trying to say is that everything that's needed to get into the SSAD would include a request founded on alleged IP infringement but that the other factors that go into the SSAD request would count as not solely being—would overcome that "solely based on" threshold, if that makes sense. I could start

again and elaborate, but perhaps we can kind of caveat or footnote our way to removing that heartburn, then I think we could probably live with the “or approval” language.” Thanks.

JANIS KARKLINS: So you’re suggesting, Brian, that we put a footnote and footnote would say that the same process should be followed in both cases, or something like that. This is what you're saying?

BRIAN KING: I'm not sure if I understood, Janis, sorry.

JANIS KARKLINS: We have a process how disclosure decisions should be made, and this initial language suggests that if that is the alleged intellectual property infringement in the content of website, then it should not be disclosed only because of that. And with this “or approval,” it suggests that it should not be disclosed only based on that this is alleged intellectual property infringement. Which means that in both cases, the same process should be followed in order to decide whether the disclosure should be done or not.

BRIAN KING: Thanks, Janis. Here's my confusion, is that when I think about the “or approval be based solely on IP, I think about, okay, so if it’s not solely based on the IP allegation, what else would be required? And then I think, oh boy, we've spent a year talking about what else is required in a request besides just an allegation, and that I

think makes this “or approval” language extraneous, right? Because all the requests have to be based on a lawful basis and you have to get accredited and go through all these extra steps. And I just think, why is this necessary if we already have in the policy a guarantee that all of those things would be present in a request and that the contracted party or whoever makes the decision needs to consider all those factors. We've already accomplished this “or approval” language via all the other work we've done.

JANIS KARKLINS: Okay. I see your point. Milton, maybe you can think of another way to get over this hurdle based on just what Brian said. In the meantime, Margie, and Alan G.

MARGIE MILAM: Hi. Yeah, I think that’s the concern that—I had the same concern that Brian raised. And really, I think that the difference is what we’re really talking about is all the other processes that lead up to the request include providing adequate support for the request.

So the way I look at it is that if you’ve gotten through the gateway, you’ve been accredited, you’ve provided proof of your trademark, you’ve made a statement explaining why you think there's allegation of infringement, that that should be fine.

So I think the reason why I have the problem with the language is that it doesn’t take into effect that evidence would have already been provided to support the request.

And once that's happened, then I don't see why there's a concern about why we would say that that alleged intellectual property infringement is not sufificent. So that's the reason why the "approval" language doesn't work for me.

Maybe if we added something like "founded on an alleged intellectual property infringement (without adequate supporting documentation)" or something. That might be more aligned with what I think Milton's trying to get at.

JANIS KARKLINS: Okay. Thank you. Alan G.

ALAN GREENBERG: Thank you. Unless I'm missing something, release of information to a URS or UDRP provider is essentially based purely on the fact that there's an intellectual property/trademark claim and related to content. That's the whole basis for UDRP/URS. And if a contracted party can refuse to provide information based on that, then that whole process falls apart. There are other cases also, but that one seems a rather blatant one which is essentially purely based on that one kind of claim. Thank you.

JANIS KARKLINS: Thank you. Stephanie, please.

STEPHANIE PERRIN: I typed it in chat, but the common term is disposition of request. If you don't want to talk about approval or refusal, then talk about

the disposition of the request, not “solely based on blah-blah.” Just trying to be helpful here. Very common in privacy and FOIA circles.

JANIS KARKLINS: Okay. Thank you. Milton.

MILTON MUELLER: Yeah, I think you can sense that we are really actually trying to come to a reasonable, balanced resolution of this conflict, and it’s very difficult to do. So I'm happy with, I think, sort of the neutralization of the term, and Stephanie’s proposal is good. The disposition of the request—you’d have to cross out “refusal or approval,” as well as “to disclose:” So, “Nor can the disposition of the request be solely based on the fact that the request is founded on an alleged intellectual property infringement.” And I don’t think you need “Without adequate documentation.”

So all we’re saying is that the fact that you have an intellectual property infringement claim doesn’t mean it gets automatically rejected or accepted. That’s fine. And I don’t see how anybody loses anything with this formulation. Really, can we just engage in a basic act of compromise and consensus here and just move on?

JANIS KARKLINS: Okay. Let me ask Brian that question. Brian?

BRIAN KING: Yes, we can. Thanks, Janis. Thanks, Stephanie. Thanks, Milton. Let's go.

JANIS KARKLINS: So we have agreement on this. Thank you very much. Ten, Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. Question ten deals with the last sentence in that box. If no personal data, no further balancing is required, and the nonpersonal data must be disclosed.

Some commenters are of the view that that sentence does not comport with the phase one recommendation of making it permissible to distinguish between natural and legal persons and have suggested that "must" be changed to "may," but there is not agreement on that from those who responded.

JANIS KARKLINS: Okay. Thank you. Again, I think it reminds me of painful conversations, and that was linked with whether SSAD should be one stop shop or this should be exclusively vehicle to disclose personal data. And I think that we also came to conclusion that if there is—together with personal data, nonpersonal data also should be put in the package, not to ask requestor go to other database to pull out nonpersonal data. But I may be wrong. Alan followed by Brian.

ALAN GREENBERG: Thank you. The phase one recommendation on legal versus natural was, what is included in the public WHOIS, public RDS system. That is, what you get without going through the SSAD, just making a query. It said the phase one recommendation said nothing about what's going to be disclosed in the process we're looking at now. And there's nothing there which says the contracted parties are not obligated to at least attempt to make a determination based on the access to the information they have on whether this is personal data or not.

So the legal versus natural is only related to what is in the public database. It is not related to what can be disclosed here and I find nothing wrong with the proposed language. Thank you.

JANIS KARKLINS: Thank you. Brian, please.

BRIAN KING: Thanks Janis. I agree with Mark SV in the chat and Alan on the phone. This should be a "must" because we're not talking about publication anymore. Thanks.

JANIS KARKLINS: Thank you. So, can we settle then on "must?" Marc Anderson.

MARC ANDERSON: Thanks, Janis. I have a little bit of concern here. I think if we're talking about only GDPR, then this might make sense. But I think also we have to be cognizant of the fact that there are other

jurisdictions and other privacy laws out there, and there are some jurisdictions that don't make or provide legal entities with the same protections and rights as natural individuals. So I'm a little reluctant to—I think the commenters make a fair point on this one, and using a "must" here might be a little bit dangerous. That may be something we end up regretting.

JANIS KARKLINS: Okay. So of course, we're talking about GDPR in principle, but we're also trying to generalize to using terminology of applicable law. So maybe we can think of some additional safeguard putting in this sentence. But let me listen Alan G and Laureen.

ALAN GREENBERG: Thank you. I have no problem if we add a clause at the end saying unless explicitly prohibited by privacy legislation, or whatever the appropriate word is there. And I'll note nothing is forcing the contracted party to determine, to pass judgment, is this personal or not? But if they know it is not personal data, then we're saying it must be disclosed.

You may have iffy situations that are gray and they're not sure, but that's not what this is saying. This is saying if it's not personal data, it must be disclosed. And if that is prohibited by local law, then fine, clearly, we need an exception for that. Thank you.

JANIS KARKLINS: Okay, so we have now proposal on the screen and maybe speakers can say whether they're in agreement. Laureen, are you?

LAUREEN KAPIN: Yes. I do agree with that proposal. I just would point out that I heard Mark's comment but I'm having a little trouble figuring out the concrete scenario that Marc is concerned about. Privacy laws are generally directed to protecting personal information, and if it's not personal, then I'm struggling to figure out what other category is going to be at issue. But that said, I would agree with this language, but I would also acknowledge that even though we are trying to at least deal with the specter of the panoply of privacy laws that may be out there, generally, we have focused on the GDPR knowing that we can't possibly anticipate all the quirks and crannies of what privacy laws are yet to be.

JANIS KARKLINS: Okay. Thank you, Laureen, for support. Stephanie.

STEPHANIE PERRIN: I have raised this many times before. ICANN has embraced the concept of adherence to the universal declaration of human rights. There's a cross-community work party working on the concept of a human rights impact assessment. That is not generally construed as applicable law. If I am a registrar and I know that there's a human rights implication that would flow from the disclosure of data, I should not be compelled by this policy to violate the human rights convention in order to basically fall to the lowest level in

countries that do not have a GDPR compliant law. I would also like to point out that many of the laws that have been passed are not enforced, and therefore—data protection laws, that is—the possibility of compliance may not be there, which would give you another loophole.

We had agreed at the beginning of this that we would have a harmonized global standard for applying this policy, that we would not suddenly drop in areas—unfortunate, less developed areas—where there is not the rule of law when it comes to human rights. Thank you.

JANIS KARKLINS: But here we're talking about nonpersonal data, not personal data of human rights defenders.

STEPHANIE PERRIN: But nonpersonal data carries human rights implications. I keep going on about this. If it's a religious organization, if it's a political organization, if it's a medical group seeking information, if it's women's rights. That's not personal information, but the individuals associated with the organization will be subject to persecution upon disclosure. We have use cases, we've brought them forward, we can bring them forward again.

JANIS KARKLINS: Okay. Thank you. Amr.

AMR ELSADR: Thanks, Janis. To be honest, I'm a little puzzled why this is an issue. As you mentioned, Janis, earlier, we had discussed previously on whether the SSAD would be used to disclose data that is already published because it is not personal data. I'm not sure why that would make sense at all, and if I'm not mistaken, that would also imply that the requestor may have to pay for the service of disclosure of information that is already publicly published.

Also, if a requestor is going to be asking for disclosure of personal data that is redacted, then presumably, they would have to demonstrate that the disclosure is necessary, which means looking at what data is already public elsewhere, not here in the SSAD, and determining that this data is not sufficient and there is a need for additional data that is not publicly available.

The last thing, I've seen a number of comments in the chat about the recommendation phase one being limited to the processing activity of publication of nonpersonal data. I don't think that was the case. I went back and took a look at the recommendation and to me the recommendation is a broad one addressing how contracted parties deal with registration data of legal persons and natural persons. It doesn't specify publication as being an issue. So I just wanted to get clarification maybe from some of the other members of the EPDP team on why they think that might be the case and how it's relevant to what we're discussing. T y.

JANIS KARKLINS: Thank you. Mark SV:

MARK SVANCAREK: Thanks. Amr, the issue is that there is lots of nonpersonal data that's redacted, and it's redacted because we don't make a natural-legal distinction. So it just gets redacted as a matter of course and now it's in the system, and there may be a case where we need to request the data that is nonpersonal.

And just as a typical example, go to Google.com or Gmail.com. And then of course, privacy proxy falls into that category as well. So there are plenty of cases, lots of cases where the data which is nonpersonal is not published and it does need to be requested, and what we're seeking here is some certainty that if you know for a fact there's no personal data in there, that you will disclose it, because if you think about the implications of it—I don't think I have to explain the implications, but if after you go through all the process and then you still want to not disclose it, I don't see what the policy is doing. So I think this is a very simple case where "must" is appropriate. I'm hoping that we can just accept it and move on. Thanks.

JANIS KARKLINS: So my question is now can we accept—or is there anyone who cannot live with the text which is now displayed on the screen? So I see no hands up. So everyone can live with that text that is on the screen. Stephanie.

STEPHANIE PERRIN: Thank you. Unless expressly prohibited by applicable law? Is that the text you're talking about?

JANIS KARKLINS: Yeah, but in conjunction with the full phrase, “if no personal data, no further balancing test is required, and nonpersonal data must be disclosed unless expressly prohibited by applicable law.”

STEPHANIE PERRIN: Okay. Let me tell you what's wrong with it. Expressly means exactly that. Not a general provisions. It means expressly with relation to the kind of data that you're talking about. Applicable law, I protested a minute ago that we were not going to fall to the lowest level in underdeveloped countries that do not have adequate rule of law. You're throwing them to the dogs. And because they would not have a proper definition of personal data. And then of course, there's the whole human rights. That means that religious organizations and all of the kinds of things that we have attempted to protect again and again under the universal declaration, political speakers, you're going to throw them to the dogs.

How many times have I raised this?

JANIS KARKLINS: So applicable law, this is the standard phrase we’re using throughout the text of the whole document. So, what would you suggest instead of expressly?

STEPHANIE PERRIN: “Unless expressly prohibited by applicable law” is a high bar.

JANIS KARKLINS: So then you're in agreement with that?

STEPHANIE PERRIN: No. Not at all. This means that nonpersonal data will be disclosed whether there are human rights implications or not. Human rights laws is very general. It does not get down to “expressly prohibited.” What you do after a balancing test, when you're dealing with nonpersonal data, is you make a determination as to whether there will be a human rights impact on your customer. That’s what you do.

JANIS KARKLINS: Okay. And if we say “unless prohibited by applicable law” without “expressly?” Would that be acceptable to you?

STEPHANIE PERRIN: I think it’s still too strong. I think you need to at least express the requirement that on principle, nonpersonal data will be disclosed—I wouldn’t say must—absent human rights considerations.

JANIS KARKLINS: Okay. Thank you. Brian.

BRIAN KING: Thanks, Janis. We can live with the language here, but I want to be sympathetic to Stephanie's concerns. I am trying, but I am not an expert in this, and clearly Stephanie is. And maybe I can ask for her to dumb it down for those of us that don't have our background in this. And I could be wrong, or I feel like I'm missing something, so I'm asking for help.

In my view, I guess, or as far as I've wrapped my head around this, if we're talking about nonpersonal data, we're talking about non-persons, and the human rights wouldn't apply to legal entities or to nonpersonal data. I think that's the connection I'm missing. I feel like there's a real concern that we could address, I just don't know how to do that, how to help Stephanie do that. So I don't think I'm the only one maybe that's missing that connection between nonpersonal data and human rights issues, but I'd love to know more. Thanks.

JANIS KARKLINS: Time is ticking. We have 12 minutes remaining on this call, and we have done today exactly five points. So at this speed, we will end up in June 30 of 2025. Alan, please.

ALAN GREENBERG: Thank you very much. I'm going to express some frustration here. We have been told innumerable times that the scope of this PDP is very limited. We have to address GDPR and we widen that to applicable privacy legislation in other jurisdictions. When a number of us have raised issues that we thought were relevant,

we're told, sorry, that wasn't listed in the PDP, it's out of scope, we cannot add things to it.

And now we're talking about widening this to cover all sorts of ills in the world, which I admit are there, but they are not within our scope. And I really don't understand the principle that we can include some things that are completely out of scope and were never mentioned, and other things are forbidden because they weren't mentioned explicitly. I've got an increasing amount of frustration with this process. thank you.

JANIS KARKLINS: Thank you. I would suggest that we leave the text without brackets as it's now displayed on the screen, and move on. And I would like to ask Stephanie to show flexibility and accept that. Stephanie, please.

STEPHANIE PERRIN: As I have said before—and this is in response to Alan Greenberg—I don't think a face-to-face has gone by without me mentioning human rights. The GDPR rests on the charter of human rights. If you want to be in court fighting this on the charter, be my guest. Fill your boots. But you're barking up the wrong tree. Pardon the mixed metaphors.

Thomas has made a good suggestion. We need to deal with this in the broader policy somewhere so that people understand how human rights law applies, how vague it is in the application, and how people will have to do a second consideration when they are contemplating the disclosure of additional—remember that this is

additional—information concerning their clients who are organizations. Thank you.

JANIS KARKLINS: Stephanie, two things. One thing is, human rights, we have one subparagraph in one of the recommendations, I think it was on disclosure, that specifically refers to human rights considerations. So that human rights is covered and that recommendation also should be taken into account when this nonpersonal data will be disclosed. So that's one element.

Second element is, as I said, with this speed, we will not conclude our work, neither in June 30 2020 nor June 30 2021. So we're heading for another two, three years of discussions. So I think if one person cannot live with the text on the screen, probably my ruling should be that that person can start writing dissenting opinion for the final report, and if everyone else can live with it, then we move on.

Thomas, please.

THOMAS RICKERT: Thanks very much, Janis. I had suggested compromise language in the chat which has received some support, and therefore might be considered. Janis, I understand that we have a time issue. I also understand Alan G's point about scope. So my intention with the compromise language was not to broaden the scope of this PDP or EPDP, but rather to express that if there are human rights implications, then these can be taken into account and then a decision can be based on that.

So that's more like a "Notwithstanding this recommendation" type of language. I leave it to staff to find the correct language for that, but that might be middle ground without us overreaching our charter and yet clarifying that human rights implications can and must be taken into account.

By the way, when we did the IANA stewardship transition, we had an actual working group dealing with human rights implications with ICANN's policymaking. So I think it's a fair point to put a reminder about that into our recommendation. Thank you.

JANIS KARKLINS: So probably then "unless prohibited by applicable law and do not entail human rights implications." Margie, would that be a way forward?

MARGIE MILAM: No. I think the concern is that essentially by doing that, you're basically saying that every single registration, before it can get disclosed, needs to be looked at manually. And that is not a position that we're willing to accept. There has to be some ability to do some automation.

But I do think that the human rights element could be automated in the sense that if there was some way to create a flag that registration involves a human rights organization or a risk of the type that Stephanie is concerned about, then at least you know that for those kinds of registrations, you have to make that kind of extra evaluation. But to have that standard apply across the board

to 300 million registrations worldwide I think is probably too much and creates an extra burden that may not be necessary.

So my suggestion would be to think about some sort of flag for human rights types—registrations that implicate human rights issues.

JANIS KARKLINS: As said, we have human rights addressed in one of the bullets. I wouldn't be surprised that in this same recommendation at the very bottom. So let me suggest the following. Staff, based on the conversation, will think whether there is any fix what Stephanie was talking about, and if they will not find anywhere to place it in the text which is on the screen, if no personal data, no further balancing is required, and the nonpersonal data must be disclosed unless prohibited by applicable law will appear in the final version, and those who are not in agreement may express it in minority opinion.

So, can we go with that? Thank you. So I think we have exhausted time for today's call. Remaining three minutes. Let me say that maybe we need to do more online conversation, because again, with this speed, we will not get anywhere anytime soon. I will talk with the staff whether there is any other method we could use to accelerate the process, but everyone needs to do the homework, and many things could be flagged already prior the meeting that we can make. If there is convergence, take out those points from the text to discuss during the call.

So I have been informed that only two groups have submitted their comments on recommendation on automation, so it's certainly not good homework so far on that point, and please, I would encourage all groups to review recommendations prior the call and submit their opposition or thoughts based on their positions. Amr, please, you have a few seconds.

AMR ELSADR: Thanks, Janis. I take your last comments to heart, and I agree. It kind of brings us full circle to your opening comments, at least when I joined the call, and I might have joined a couple of minutes late. But I honestly believe that adding a call on Tuesdays regularly for the next few weeks and also considering the additional homework that will be assigned as a result of additional calls and the tighter time frames or deadlines that we will need to meet is going to only make things more difficult, not easier.

Speaking for myself, the past couple of months have been challenging for sure, and I'm very concerned about what the outcome of an additional call every week—whether that's actually going to help or whether it's going to make things more difficult. So I just wanted to voice that concern. Thank you.

JANIS KARKLINS: Thank you. Again, I'm trying to find a way how we can get final report out in reasonable time. So I can only repeat that my availability ends on 30th of June, which means that if we're not done with this, either GNSO needs to find a new chair or each of the team members may take up chairmanship on rotational basis

and then go through without finding chair. But nevertheless, we need to go through all the recommendations. and if we do it on the fly, looking at the recommendations and comments and questions and comments related to those recommendations at the time of the meeting, of course, then we are not prepared and it takes much longer.

so if for instance everyone does homework before the meeting, and if there is a convergence of opinion, staff can do their job and not put questions for the consideration of the team, but if homework is not done, then of course we need to review everything during the call.

So that's the reality, and all I can say, please do homework, come o the meetings, prepare so that we can proceed swifter.

With this, I would like to thank all of you for participation, and next regular call is next Thursday. We will continue examining recommendation six, seven and then also recommendations that have not been considered by then by the EPDP.

And for those who are interested in talking through the cost estimate of SSAD, please join the call on Tuesday 12th May at 2:00 UTC.

With this, in absence of further requests for the flor, I would like to thank all of you, wishing good rest of the day, and declare this meeting closed. Thank you.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines, and have a wonderful rest of your day.

[END OF TRANSCRIPTION]