ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Thursday, 19 December 2019 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/WYEzBw
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, and good evening. Welcome to the GNSO EPDP Phase 2 Team meeting taking place on the 19th of December, 2019, 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 then telephone, could you please identify yourselves now?

Hearing no one, we did have listed apologies from Georgios Tselentis, but, as you see, he has joined on the telephone. He'll be able to stay on for about 30 minutes. At that time, he will formally assign Olga Cavalli as his alternate. Alternates not replacing a member are required to rename their line by adding three Z's to the beginning – it does sound like someone has an open line. If I could just please remind everyone to mute.

Back to the alternate, if I could just remind all alternates to put three Z's in the beginning of their name and, at the end, their affiliation-alternate, which means that you're automatically pushed to the end of the queue. To rename in Zoom, hover over your

name and click Rename. Alternates are not allowed to engage in the chat, apart from private chat, or any use other [Zoom room] functionalities, such as raising hands, agreeing, or disagreeing. As a reminder, the alternate assignment form must be formalized by way of the Google assignment. The link is available in all meeting invites towards then bottom.

Statements of interest must be kept up to date. If anybody has any …

UNIDENTIFIED MALE: Give us a second. I believe we've just lost Terri.

UNIDENTIFIED FEMALE: Yeah. One moment, please.

Thank you, Janis. She was at the end of her introduction, so we will go ahead and turn it over to you.

JANIS KARKLINS: Thank you very much. Good morning, good afternoon, and good evening, everyone. Welcome to the 37th call of the team. It seems this is the last one in this year. I would like to see whether the proposed which is now displayed on the screen is the one we could follow. Any objections?

I see none. In that case, we will follow the proposed agenda. The first item is a quick update on the face-to-face meeting in Los Angeles. Berry, please go ahead.

TERRI AGNEW: This is Terri. I'm actually back. Sorry about that. I just want to remind everyone that we have about seven folks who have not booked their travel for the face-to-face L.A. meeting. If I could please encourage you to book your travel as soon as possible. All e-mails from ICANN Travel have been sent out. If you don't have yours, please reach out to me – again, this is Terri Agnew – and I'll help work through that process.

In addition to that, I just wanted to remind you that are meeting schedule will stay the same format as the previous meetings. So, on your arrival date, known as Day 0, we're going to have our Welcome cocktails and snacks and everything more than likely at the hotel. But that's still a work in progress. Of course, you'll be sent information on that, so please plan for that.

In addition to that, after Day 1, we'll have our team dinner. We're working on a location for that as well. But, again, you'll be notified. Please plan to stay all three days with a reminder that the last day, on Day 3, we are ending at 2:00 P.M. local time, so you are able to catch flights later that evening if needed.

Back over to you, Janis. Thank you.

JANIS KARKLINS: Thank you very much again. Now let us to the next – sorry. Any questions? The team dinner is on Monday but the reception on Sunday. I'm asking Mar[c]'s question. Any other questions?

If none, then let me go the next sub-item, and that is the Legal Committee updates. If I may ask Becky to provide this update.

Becky, are you on the call?

That's maybe not the case. Maybe then Caitlin can give us an update.

CAITLIN TUBERGEN: Hi, Janis. I can give a quick update from the Legal Committee. The Legal Committee met on Tuesday. Shortly, there will be three questions that the Legal Committee has approved to send to the Plenary Team. We'll be sending them out in short. There's a question that deals with reverse WHOIS lookups, there's a question that deals with pseudonymized e-mail addresses, and there is a question that deals with legal versus natural and WHOIS accuracy. Again, the Legal Committee has reviewed those questions. They are still in the process of reviewing several questions that various team members have put forward with respect to the Priority 3 items. We will continue reviewing those into the new year. The three questions that have been approved will be sent to the plenary for its review.

Additionally, summaries of the Phase 2 memos that the team received during the face-to-face meeting in Los Angeles will also be sent to the plenary team shortly.

Thank you, Janis. That concludes the update.

JANIS KARKLINS: Thank you, Caitlin. It's all for Christmas reading. So thank you. Any questions or comments in relation to the Legal Committee updates?

I see none. Then the next subitem is the status of our work. We have on the screen the table. As you see, many things have turned green with just a few yellow windows. Three of them I hope we will be able to close today. These are three substantial agenda items that we have on our agenda. Then there are one or two outstanding, but those depend a little bit on our discussion and inputs received from the [outset].

Let me also brief you on the latest developments. Yesterday I distributed two e-mails to the mailing list. One was in relation to the communication that ICANN org put out on the 17th, indicating that the first informal communication has been received from the Belgian Data Protection Agency in writing to further discuss to proposed UA model. I propose that everyone reads this communication and maybe we can discuss, if need be, during the first call of the next year or the second call of the next year.

The second thing was I received an e-mail from Goran in response to my e-mail that I sent with your consent in relation to the assessment of cost involved in building and running a system that we're talking about.

Again, since this communication came in only yesterday, very close to the call, I suggest that we digest this information from the e-mail and discuss it one of our next calls.

Today, we received, from ICANN org, also a comment on the implementability of "should." This was the question which was asked at ICANN org a few meetings ago. In essence, the answer is it is very difficult to implement "should." The preference would be "must." Again, this is something that we need to discuss once we'll get to those outstanding issues in several building blocks where we had difficulty in agreeing on the term "should" versus "must."

With this, I wonder whether there is anyone who has any questions or remarks.

I see Marc Anderson's hand up. Marc, please go ahead.

MARC ANDERSON: Thanks, Janis. Quick question. On the communication from the Belgian DPA, you said we received a first communication to the Strawberry letter. Does that imply that ICANN is expecting more communication or additional follow-up on that? Or can we expect that to be the only communication that's going to be received on the Strawberry letter?

JANIS KARKLINS: I read exactly the same post from ICANN with a link to the letter, so my understanding or my reading of the letter is that there was an invitation to continue the conversation and provide some additional elements. Then we can expect a formal communication. So this is my understanding.

But, if Georgios is on the call, maybe, since Georgios is a closely associated with this process, Georgios, you would like to say a few words in this respect and maybe explain what we will be the next steps and how it will work ultimately. I do not want to put you on the spot, but, Georgios, if you could speak a little bit about it, it probably would be helpful. Georgios?

GEORGIOS TSELENTIS: Yes, I'm here. Can you hear me?

JANIS KARKLINS: Yes, Georgios, we hear you very well.

GEORGIOS TSELENTIS: Okay, thank you. You are right, Janis. That was the first letter sent by the Belgian DPA. We thought it was publicly [released] from ICANN org. Then we had the response of ICANN org. This is, to my understanding, an invitation to provide more information also regarding the content of the model and how this is compliant with the policy that was developed to conduct GDPR according to the policy that we developed in the EPDP.

So my understanding is that there's going to be a round of, again, a formal technical meeting between ICANN org and the Belgian DPA before having a formal reply to the policy guidance, which was sent out in the original letter.

So our reading was that – I'm talking here with the hat on of the [inaudible] – there is a need for more information. There's many

issues which are developed under also the EPDP in order for the Belgian DPA to make [inaudible] there is normally a DPA which is taking the lead and introduces the [subject to the Board] before having a formal reply.

But we are still at the stage where the Belgian DPA, which is a penholder for this process, is seeking more information. In my understanding, in the beginning of January, there are seeking to have a technical meeting to have more information.

This is as much information I have from my side. Thanks.

JANIS KARKLINS: Thank you, Georgios. I hope that explains and answers a few questions that were on Marc's mind.

I see Amr's hand up. Please, Amr, go ahead.

AMR ELDSADR: Thanks, Janis. I do note that you said earlier that we would discuss the substance of the letter from the Belgian DPA at a later time, but I did want to highlight one really important takeaway from that letter. Irrespective of the model that we end up using for the SSAD, the roles and responsibilities of controllers and processors [can't] be designated. They're based on a factual assessment of how data is processed, by whom, and who requires this processing to take place. So I thought this was very helpful input to our work, at least. Noting that we're not going to get into the substance of this letter, I think this is something we should, as a

team, keep in mind as we try to make progress on our policy recommendations, even during today's call. Thank you.

JANIS KARKLINS: Thank you, Amr. I see Mark Sv. Mark, please go ahead.

MARK SVANCAREK: Thanks. I thought the more interesting feedback in the letter, which [from] Amr notes it actually derives from, was that they seemed to think that this would be a joint controller relationship. I don't know if anybody else perceived that. That was the way I read the thing. I felt that a weakness of the original Strawberry memo was that it didn't lay out who they thought the controllers would be. It was, "If this, if this, if this." It seemed to me like we could probably set that equivocation aside now and just proceed with the assumption that, however the process is divided up, it's divided within the framework of a joint controller agreement. So I think that's a good clarity to get as well. Thank you.

JANIS KARKLINS: Thank you. I think the ICANN org liaisons are taking notes of this brief conversation. We will provide further clarity to the Belgian DPA.

I see Milton's hand is up. Milton?

MILTON MUELLER: I just thought that the remarkable thing about the letter was the sentence near the beginning: "It is on the role of the supervisory

authority to validate or approve the suitability of organizational or technical measures which are being considered by a controller as part of its compliance obligations." To me, that's a pretty direct statement that we need to stop nagging the DPAs about what we're doing and just design a system that complies with the law.

I have, as some of you know, been questioning the point of this back and forth between ICANN org and the DPAs and the meaning of the Strawberry Team for some time. To my mind, this letter just validates those questions and encourages us to not wait for further feedback and just continue trying to make an SSAD that is compliant. Thank you.

JANIS KARKLINS: I think this is our aim, indeed. Mark, your hand is up again. Mark Sv?

MARK SVANCAREK: I just wanted to respond to Milton a little bit. I thought that the purpose of this exercise was to determine what the law said: that there were some feelings, that there were some ambiguities, in certain configurations that needed to be clarified. So I think saying that we just needed to build a policy that is compliant with the wall I thought was what we were trying to do, actually. So I thought that this was a vital portion of trying to come to that assessment. So I don't see it as a conflict, actually. Thanks.

JANIS KARKLINS: Thank you. There's no further immediate requests for the floor, so I take it that we will continue this conversation in one of the next meetings (the first or second).

Now we can move to the next agenda item, which is the building block on user groups. If I may ask [inaudible] if we can get this on the screen. We have now on the screen the proposal from staff.

Margie, your hand is up. You will speaking on the user groups or you have a comment on the previous item?

MARGIE MILAM: A comment on the previous one.

JANIS KARKLINS: Please go ahead.

MARGIE MILAM: Given the meeting that ICANN org will have with the Belgian DPA next week, is there any value in at least providing some input from the EPDP on what elements should be presented to them? I think the letter clearly is asking for questions and more details on the safeguards and the aspects of the model. In order to avoid a situation where it'll get not answered again because there's no adequate information, is there a possibility that we could provide input to ICANN staff on what elements to highlight based on the building blocks we've already worked through?

JANIS KARKLINS: Maybe we need to ask the ICANN org liaisons about whether they expect some feedback from us. We will discuss the issue, as I mentioned, in one of the meeting. At least I will put that on the agenda of either the first or the second meeting of next year. If there will be interest, then probably the ICANN org liaisons will take notes and provide all the information to the Strawberry Team. Or we can invite the Strawberry Team to join if that would be the wish of the team itself.

On the screen, we had a conversation about [building groups] on a number of occasions. We tried to establish the non-exhaustive list. It appeared to be very difficult.

The second sentence that we see on the screen – the longer paragraph – I understand was on the table before, but, after receiving comments from different groups, staff is proposing to use a simple formulation in three lines.

But let me make sure that my explanation and recollection is right. Caitlin, can you confirm that we can work only on those three lines today? If we agree then that would be our task.

CAITLIN TUBERGEN: Thanks, Janis. To clarify, yes, that is correct. The yellow, highlighted text is the text that appears in the initial report. The text below it follows our last meeting – what Berry is highlighting right now – where a couple of folks had noted that it would be helpful to include a non-exhaustive list of user groups. So we went ahead and proposed some text, which is now in brackets, for discussion. Thank you.

JANIS KARKLINS: Okay. If you read the upper sentence, it's basically the first sentence in the second paragraph at well. So let me try then to work on the basis of the longer paragraph, which is the second paragraph. Then we will see whether we can get something out of it.

Thomas, please, and Hadia.

THOMAS RICKERT: Thanks very much, Janis. Hi, everybody. I would have hoped that we made more progress in the legal team with the response to our question of what eligible requester groups could be. But, in the absence of that, I would kindly ask to include Internet service providers and abuse departments in that list in the text because the ISPCP has asked me to put that in explicitly so that this is not being forgotten as we move on and work on that [accreditation] policy. Thank you.

JANIS KARKLINS: Okay. Let me take a few hand and then see whether that is what we want to pursue. Hadia, please, followed by Laureen.

HADIA ELMINIAWI: I would like to quote a few lines from the Belgian DPA letter. On the second page, the third paragraph says, "[If] it's expected that such a policy would describe who gets access to what under what conditions for how long …" Then it continues to say, "From a data

protection perspective, such elements will be extremely important when assessing whether the model which is ultimately developed complies with the requirements of GDPR or not.

So my understanding from this is that we do need to mentioned who gets access to what and who, I assume, is the user groups. Or do we have another [inaudible] somewhere else? [I don't know.] Thank you.

JANIS KARKLINS: Thank you, Hadia. I think we have the description of who has access in other building blocks. So each individual or each organization [that] should be accredited gets access to SSAD. In my view, if I can abuse my authority of the chair, user groups may be, at least in configuration with what we have now, useful only for [facilitating] accreditation because there is no distinction between [inaudible] the processing of the request.

Let me take Laureen, whose hand is up. Laureen, please go ahead.

LAUREEN KAPIN: Just quickly I would add civil law enforcement as well as criminal law enforcement and consumer protection authorities. I actually would add data protection authorities for that matter.

JANIS KARKLINS: Thank you. We have proposals from ISP and the Internet service providers and now data protection authorities and civil and criminal law enforcement.

Berry, can you scroll down a little bit to the next page, which we already tried once and couldn't get to the bottom of the list?

Berry, please scroll down the screen.

Berry, do you hear me? Or who is controlling the screen?

BERRY COBB: This is Berry. This list, yes?

JANIS KARKLINS: Yeah. On the next page, if I'm not mistaken, there is already one list that we looked at and couldn't agree on.

JANIS KARKLINS: So—

JANIS KARKLINS: In the same document.

BERRY COBB: Right. I'm in the same document. I'm on Page 2. Is your computer frozen maybe?

JANIS KARKLINS: Ah, sorry. Yes. I am looking on my computer. So you see we have from A to R. Maybe we simply can important this list instead of now redefining because we are talking about a non-exhaustive list.

Let me take Marc Anderson and then Milton and then Laureen again. Or Laureen's hand was an old one. Marc Anderson, please go ahead.

MARC ANDERSON: Thanks, Janis. I was going to make a comment similar to what Marika said in chat. Hi, Marika. Please note that this is a non-exhaustive list. it does not mean that something not mentioned is not included. I'm actually not sure what we're trying to do by taking the list we didn't agree on before and including it in this text. This seems crazy to me.

I like the initial two-sentence language. It says that the accreditation authority may include user groups and categories. I think that gives the accreditation authority flexibility to create whatever user groups they want, which seems like the best approach for us. But now we're basically trying to recreate what we didn't agree on before, taking the original language and trying to make an exhaustive list of user groups and categories. I'm not even sure what problem we're trying to solve by including in the policy a list of all these user groups and categories.

So maybe somebody can help me out here, but I think the initial language provides much more flexibility here. It allows the accreditation authority to create … It says "user categories and

categories." I think it's intended to be "user groups/categories." This language seems more flexible and a better way forward. But, if somebody can point me to what problem we're trying to solve by adding all these user groups, I'd be happy to hear it.

JANIS KARKLINS: Thank you, Marc. Now we have two options, as I see it. One option is to go actually for the first very short version without even attempting to list any of the groups – just what Marc said. The second one is to work through and add every Christmas decoration on the tree. Then it will be [wrong] and not nicely readable.

Let me take Milton and then Alan G. and Margie.

MILTON MUELLER: Well, I pretty much agree with everything that Marc said, except that I would never call anybody crazy or this list crazy. I just think it's poorly thought out.

I think I can amplify. I think Marc has made a pretty much cut-and-dried case for why we shouldn't have this list, but I want to identify some of the conceptual problems that went into this list. If the job here was to create a set of categories, the level of overlap between these categories is a nightmare, from somebody who has a tidy sense of information systems' ontologies. So is, for example, Google a social media company or a search engine? Is it a non-law-enforcement investigator? It could be all three of those things.

I would urge us to stick with the simpler language and also to keep in mind that we need, as Marc said, to understand what problem we're trying to solve. So, to my mind, the most important categorical distinctions we have are between law enforcement investigators or law enforcement agencies and private non-law-enforcement. In fact, probably the whole thing might be reducible to that in terms of what type of a user group you're dealing with. An intellectual property owner can be investigating a phishing scam, which might make them a security investigator.

I just don't understand the point of creating these overlapping, confusing groups. I just don't understand what it's accomplishing. So I'm definitely hoping that we can just delete that whole list and even remove a few categories from the shorter list. Thank you.

JANIS KARKLINS: Thank you. I think the building block was put [on the list] at the beginning of the exercise. So we had this conversation on whether there would be any distinction of creeping of requests based on where or by whom they [originate]. So, currently, it seems to me that there will not be any difference in the processing terms of any request.

In my view, as outlined in the proposal we are discussing now, the only value of the user groups to facilitate accreditation. In case – this is an implementation question – there will be one or two or three identity verification organizations, then they may be specializing in a certain type of clientele. Then these groups may indicate which of those organizations would do accreditation and identity checks for that purpose.

Actually, I would even argue further that maybe we simply need to formulate one sentence for accreditation, if you are in agreement that the accreditation authority can create a list of user groups to facilitate accreditation. And that's it. That would be up to them.

But, since I am not the who one decides, let me take four requests in order: Alan G, Margie, Mark Sv, and Thomas.

ALAN GREENBERG: Thank you very much. I guess I'll agree with everyone who speak before that this long list is going to maximize our work instead of help it. For instance, including, as a class/user group, search engines? I understand we're using the phase "could include," but we're almost maximizing the amount of work we have to do by including things which will not really be accredited users as such because, if we're saying any search engine can access data under some conditions, I think we're just generating work for ourselves.

In addition, I believe we ended up with two kinds of accreditation – one identification and one … I can't remember what word we used, but it was essentially saying what the purpose is for your use. I think the user group is going to be most useful for the latter one. Among other things, it will give you some idea of who to go to for accreditation by – how do you recognize yourself and who do you go to is going to more of a guidance to the user to know where to go. Also, it may well include a pre-prescribed list of commitments that the users make.

So I think we want to keep this one as general as possible right now and, under the accreditation, try to understand better how user groups will facilitate the problem. Otherwise, I think we're creating work for ourselves, which may not be beneficial at all. Thank you.

JANIS KARKLINS: Thank you, Alan. Margie?

MARGIE MILAM: I think the concept of user groups is useful because it does identify the likely types of requesters that would use the system. So I think it helps in identifying who can verify their identity.

But really the issue that's most important for the BC is the purposes. I think, once we've got assurances that the purposes include things that are covered by some of these user groups, we'd probably be more comfortable with not having such a detailed list. But having the shorter list that ICANN proposed is not bad because I think it at least gives comfort to our stakeholder group that these types of users will have access to the system.

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: I agree with most of what was said by most of the people before us, so I think we're making some progress here.

I had a thought regarding the idea of overlapping categories. I think that that's okay. You know that Microsoft has many of these categories, and I think that it's fine because each of these categories ultimately goes to what sort of authorization that you'll have. Now, the accrediting body probably doesn't have any involvement in that, but, to the extent that it was identified at the time of accreditation, it could be of benefit to the authorization provider. So I think that that's not inherently a problem. Thanks.

JANIS KARKLINS: Thank you. Thomas Rickert, followed by Alan Woods.

THOMAS RICKERT: Thanks very much. To be honest, I have an issue with some items on the list as well, not only in terms of overlap but also in terms of clearly defining who belongs to that group. What I think we need to do is make sure that – maybe it can be in the implementation advice – when the implementation policy is crafted, all potentially eligible groups that our group has identified are actually being worked on. Whether they will all make it to the final list of accredited parties is a different question and requires more legal assessment in particular. But what I could very badly live with is a plain text without a list with examples that would not include the network operators/Internet service providers. So, if you want to strip out the entire list, then at least we should give implementation advice that all items that we listed needed to be investigated thoroughly.

JANIS KARKLINS: Okay. Finally, Alan Woods?

ALAN WOODS: Thank you, Janis. I just want to go back to something that Margie said there: that we're creating this list because the intention is to provide comfort to certain people. To be perfectly honest, we're here to make a community process and it should be what is best for the community, not best for just what you're talking about. I think we've already discussed and very clearly pointed out the fact that it's easier from a recommendation point of view to leave this list as an open-ended one that should be created based on what the actual provider/person who's going to be making and allocating these things [inaudible] for them to identify users based on very obvious things, such as the request they receive.

Can we just also point out that anybody can make a request? Just because you're not on the list doesn't mean you can't make that request. Therefore, this concept of that you will be excluded since just a little far-fetched, to be perfectly honest. It's not really helping us move forward in this.

So I support the fact that we should make this much cleaner and much simpler. I personally think the list is not necessary. But, as [inaudible] said there, if there's going to representative examples and [you] make it clear that that is what it is, it should be that. But let's be clear on what we're trying to achieve here, and that is that … Yes, I agree with Hadia. We have to have clarity when it comes to the privacy policy, but the privacy policy is something that, again, should be written by the person making the disclosure or the actual SSAD, depending on what we're talking about. That's

for that person to decide as the controller. It's not for us to tell them what they are going to be doing. We need to be clear that we're not stepping on the legal obligations of the controller. We're here to recommend, not to push them back into a legal corner.

So I just want to be very clear that we have to be careful there.

JANIS KARKLINS: Thank you, Alan. Let me ask you one question. And, Alan, if you could – yeah, thank you for lowering your hand. I did not hear anyone speaking about the use of user groups outside the accreditation.

Let me formulate a question. Is there anyone who thinks that user groups would be used for other purposes than accreditation? If that is so, please raise your hand and then explain where they can be used outside accreditation.

Okay. There are no hands. So then my next question is, would you agree that we would ultimately delete user groups as a building block but would add one additional paragraph in the accreditation building block in relation to user groups? Is there anyone who opposes that proposal?

Alan Greenberg, please?

ALAN GREENBERG: Thank you. Ultimately, you may be right, but I think we need to keep it as a placeholder until we do that other work. But I would

like to see a very simplified version closer to what we started with, not that exhaustive list.

JANIS KARKLINS: Thank you. If you read the current proposal, whether long or short, it is written for the building block. But when we will put those building blocks one after another and would read the text in one go, this text which is proposed would need to be modified anyway because it suggests that the EPDP team expects that the question of user groups will be addressed through the accreditation policy. So our accreditation will follow this building block if we keep the user group building block or such, or recommendation. Specifically, all requesters will need to be accredited, which the accreditation building block suggest, and accreditation will include identity verification, which may use the user groups or categories.

So where I'm leading to is that, in reality, we could add one sentence in the accreditation building block, suggesting that the accreditation authority can decide to use user groups to facilitate the accreditation process, or something along those lines. So that would be my comment here.

Milton, are you in agreement with me?

MILTON MUELLER: Yes, I am. I think that's a brilliant idea that gets us out of this whole we've been digging, where people think, if they're not on the list, they won't be accredited, which I think is an absurd fear. But apparently people have it. Obviously, to me, particular categories that accreditation providers stuff applicants into is an

implementation detail and shouldn't have anything to do with who gets access to data in the end and who doesn't, except possibly in the case of law enforcement agencies. So I think that's a very good solution: to provide minimal guidance here, to consider this as part of the accreditation building block. I think that's what we should do. Thank you.

JANIS KARKLINS: Thank you, Milton. Is anyone conceptually in disagreement with my proposal? Conceptually.

Okay. So then I would propose the following. For the first reading of the initial report, staff would formulate one additional line and we will make it distinctively clear that this line needs to be reviewed and preliminarily agreed to by the team. Then we will see whether the non-exhaustive list we should add to the implementation guidance of the accreditation building block or we would simply leave this to the discretion of the accreditation agency or accreditation authority, whoever that will be.

If that would be acceptable, then we could move to the next agenda item and we would agree on the final formulation, a very simple one, during the next call.

I see Dan's hand up, and then James and Franck. Dan, please go ahead.

DAN HALLORAN: Thank you, Janis. I'm just trying to follow along, just to make sure I understand from an implementation point of view what's being

discussed. I'm a little concerned we're talking about various different people – the accreditation authority, I think you said. Somebody said authorization provider, accreditation provider. I'm just not understanding, like, when would this happen? I want to make sure you're not saying that ICANN org will somehow come up with a policy at some point that will define these groups [inaudible]. Thanks.

JANIS KARKLINS: The accreditation building block, Dan, is stabilized. I'm not saying that it is finalized, but it is stabilized. I maybe used the wrong term, but we have a clearly defined process of accreditation. We would simply add the notion that the accreditation authority – where that will be – may use user groups in order to facilitate the accreditation process, or something like that. There is no difficulty or, let's say, problematic issue for implementation of this policy recommendation.

James Bladel, please?

JAMES BLADEL: Thanks, Janis. Generally, I think I'm okay with leaving this open and creating some room to navigate for the accreditation entity. My only proposal here – I haven't cleared this with anyone in my group, so I'm just putting it on the table for discussion – is I'd be a little more comfortable if there were some requirements for transparency into this process, which could include, for example, some periodic reports on how many entities apply for accreditation, how many were granted, how many were rejected,

why, and so forth. I know that creates a little bit more work, but, in order to build that sense of confidence in this function being carried out according to, I think, what we're trying to do here, I think we need some degree of visibility into the process. Thanks.

JANIS KARKLINS: Thank you, James. If I may ask maybe Marika to quickly look to the agreed-to accreditation language and pull out appropriate things and put it in the chat in response to James' request.

Franck, please?

FRANCK JOURNOUD: Thanks, Janis. Quick question. I may have missed this. I wasn't clear on what you were proposing [as a] compromise and move forward, including also the point that I think Margie and [inaudible] the IPC make. For us, this question of user groups is closely linked with that of purposes. We want to make sure that we're going to have satisfaction or an agreement on purposes if we're going to – not reach an agreement on purposes now, but we want to make it clear that will need to have agreement on purposes first. That's the way we move forward off of this user group issue now.

JANIS KARKLINS: Thank you, Franck. This is exactly what I'm saying: that we will look to the final agreement on the language when we will do the first proofreading of the initial report. This will be in indicated – that

we need to concentrate on that specific language because it was put in without final approval by the group.

If that would be acceptable, then we would move to the next agenda item, which, if I'm not mistaken, is Building Block B: Purposes.

FRANCK JOURNOUD: Thank you.

JANIS KARKLINS: I see no objections to this proposal. In the meantime, we will see whether we can pull out appropriate text from the accreditation building block in response to James' comment.

Now, the next – sorry. According to our agenda, the next item is acceptable use policy. Purposes come afterwards. I think we can follow the agenda because my intention is to get through the agenda today. So acceptable use policy. Again, if I may ask Caitlin to refresh our memories. Now text is on the screen. We have, I think, two outstanding issues in this text. It is H and I. What follows after yellow staff support team comments is already from our previous exercise. Basically, we would need to concentrate exclusively on Subpoints H and I, since everything else had been already stabilized during the previous meeting.

Am I correct, Caitlin?

CAITLIN TUBERGEN: Yes, Janis, you are. I will note that, in terms of H and I, we did receive one comment from NCSG, which is then margin to discuss.

JANIS KARKLINS: Thank you. Let me see. This suggests that probably we need to simply refresh our memories, so we'll read quickly. "The entity disclosing data must only disclose data requested by the requester, must return current data, must process data in compliance with applicable law, must log requests where required by applicable law, must perform a balancing test before processing, must disclose to the registered name holder on reasonable requests, confirming the processing of personal data related to them, where required by applicable law, and must provide a mechanism by which the data subject may exercise its right to [erasure.]" So that was agreed to.

Now, on confidentiality of the disclosure request, the EPDP team will consider further once it is decided who is the authorizing provider. But the EPDP has acknowledged that the nature of legal investigations or procedures may require SSAD and/or the disclosing entity to keep the nature or existence of these requests confidential from the data subject.

I think that we should start our reflection on the text, starting with, "The EPDP team has acknowledged that," since the previous one is simply supporting text. Maybe I will start with Marika, followed by Amr. Marika?

MARIKA KONINGS: Thanks, Janis. I just wanted to provide a little bit more context, as I think it's a while ago that people probably have looked at this building block and the language you see here.

In H, you may recall there was quite a bit of discussion. I think there were several language suggestions there that were made. I think a small group even worked on that. I think, after the conversations, people felt that this may not be one that the group could answer until it was known who would be the authorization provider. So what staff did was [state] that as a placeholder: that this is an item that the group did think about but we'll only be able to define what the requirements are once it has decided on the authorization provider.

Similarly, on I, there were a couple of suggestions there. We had a bit of back and forth. From a staff perspective, we believed this was the last version that the group landed on. If I recall correctively, I think it was language that Thomas suggested, where several saw this summarized or summed well what I think people tried to convey with the different versions that were suggested. So, again, staff put that one in here. At least we felt, based on the conversation, it seemed the support from most as conveying the point that people wanted to make.

So that's why we're flagging these two specific items for discussion and confirmation that people still are comfortable that this is language that can go into the initial report. I hope that's helpful.

JANIS KARKLINS: Thank you. It is, Marika. Also, if we would, again, try to push the decision on this subparagraph until the time when we will have a full understanding of who will be the authorization provider, then of course it is simply kicking the can down the road.

I think we know that there might be, in reality, two options. One is that the disclosure decision is made in the centralized way at the central gateway by a central gateway operator. Or the disclosure should be made at the level of contracted parties, which means we would have 2,000+ disclosure points. In the worst case, we can think providing two sentences, one in relation to if there is a central decision-making point, and the second on if there is a decentralized decision-making option.

With this, I would like to invite Amr, and Mark Sv will follow. Amr?

AMR ELSADR: Thanks, Janis. I wanted to note two things. Frist, the NCSG comment here, which is specific to this portion in H, is actually repeated three times in this building block. So, if we do agree to make the change, then it needs to be made here as well as to other sections in the same amount of building block.

The other point is that, to me, the proposed edit here is somewhat of a friendly amendment, so I'm hoping it won't be too contentious. The acknowledgement here is that there may be situations where the confidentiality of the existence of an investigation is required. So, when we say that it may be required, that in itself means that it will apply to some investigations and not to others. So adding the word "some" here only reinforces that and doesn't really change

anything. So I think it just makes I clearer. So I hope it will be viewed as a friendly amendment. Thank you.

I should probably add that this independent of who the authorization provider ends up being, as far as the NCSG comment is concerned. Thank you.

JANIS KARKLINS: Thought, in all honesty, I do not see a difference in the decision-making process itself with whether that is a centralized decision-maker or a decentralized decision-maker because, in the centralized [model], there will be 2,000 individual decisions anyway.

Let me take Mark Sv and then Brian.

MARK SVANCAREK: I'm sorry. I put my hand up now, anticipating that it'd still be up when it got to I. So actually I'm fine with H. H is good as it is, but my hand was up for I. I apologize.

JANIS KARKLINS: Okay. Thank you. Let me see if Brian is good with H.

BRIAN KING: Thanks, Janis. My hand is up for I also.

JANIS KARKLINS: Okay. So may I take it that H would read that the EPDP team has acknowledged that some legal investigations or procedures may require SSAD and/or the disclosing entity to keep the request confidential from the data subject? In that formulation, as I read it, can I take it that this is acceptable to the group to go forward?

I see no requests. Then we will stabilize this. Berry, if you could delete the initial thing and we start the sentence with, "The EPDP team has acknowledged that …"

And we have I, which reads, "Wherever the circumstance of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, then this shall be taken into account during the decision-making."

Mark Sv, Brian, and Alan Greenberg.

MARK SVANCAREK: Thanks. I agree with I in general. I think that increased risk needs to be defined. I think that there is specific language in GDPR that explain what we're going for here. I've been looking for the citation. I'm sorry. I think that Stephanie problem has it memorized. So I think we recall what we're talking about, that there's certain people and we're going to be at risk because [they're] advocates or [they[re] children or something like that. I would like to have a reference to that language in the GDPR. I think it will clear this up. There is a risk that simply saying "increased risk" will be misinterpreted when we get to implementation. Thank you.

JANIS KARKLINS: Okay. Can we think of putting an asterisk and footnote and, in the footnote, put out a provision of the GDPR explaining what that increased risk is?

MARK SVACAREK: I think that would work for me. Thanks.

JANIS KARKLINS: Okay. Brian King, please?

BRIAN KING: Thanks, Janis. I have two points. One is along similar lines as Mark's. I'm happy with the asterisk and looking into precise language. I do think that this is only half of the story. If there's a balancing test, then we should be clear about the risk for the data subject. That certainly goes into the balancing test. If the risk is prosecution, criminal or civil – in particular civil litigation – then that would actually be a factor that would weigh in favor of disclosure. But I think maybe we don't need to get into that point here if we don't have a good answer for my next question, which is, what is this language doing here? We're in the AUP section of the building blocks, and this looks like something that belongs in the disclosure building block, where we talk about what types of things need to be factored in and how the balancing tests should be done. So I'm not even sure that this belongs here. So I'm a little confused about why this is here, and I suggest that this concept is good and, one, we need to be clear about it, and, two, we need to understand if it even needs to be here.

JANIS KARKLINS: Okay. This building block speaks about acceptable use policy. I think, if we can agree on the concept, then moving agreed-to concepts around would be reasonably easy once we will read the text in its entirety. But your concern on the proposal is noted.

Let me take Alan Greenberg and then Laureen. Alan, please go ahead.

ALAN GREENBERG: Thank you very much. My hand was actually a slow one for the previous item. Just a clarification. I assume the words "legal investigation" mean an investigation by law enforcement as opposed to legal versus illegal investigation. Assuming that's correct, I just think we need slightly different wording. I'm happy to leave it to staff to say that this is an investigation by law enforcement or whatever the right words are as opposed to something which is in fact legal because an intellectual property request is legal versus illegal, but I don't think it's the one we're talking about here. So I think we may need some clarification. Thank you.

JANIS KARKLINS: Thank you, Alan. I think this confidentiality notion came from the GAC law enforcement. But, yeah, probably you're right.

Laureen, please?

LAUREEN KAPIN: Also on the issue of confidentiality, I agree that not every law enforcement request necessarily is going to need confidentiality. Some investigations or matters are public, in fact.

But, on the other hand, I think there should be a defined process for either having some sort of presumption of confidentiality, because I do think the majority are going to involve that, or defined procedures where, once confidentiality is requested, then that must be provided.

So I don't object to the concept that not all investigations will require confidentiality, but there was to be some sort of piece that, when confidentiality is requested, it must be given, or a presumption of confidentiality unless there is a statement made that confidentiality is not required.

JANIS KARKLINS: Okay. I regret that we are jumping from one place to another, but, James, you're coming in for the last conversation on confidentiality or for Point I?

JAMES BLADEL: Thanks, Janis. My comment is on confidentiality.

JANIS KARKLINS: Okay. So then we will drop I for the moment and we'll continue with confidentiality. Please go ahead.

JAMES BLADEL: Sorry to backtrack. I admit that, in trying to figure out if this duplicative or if it's pushing off of the work that Chris Lewis-Evans and I did as a small team … I just want to reiterate that this SSAD system that we were designing is not the only mechanism for law enforcement and that, if law enforcement investigations require confidentiality and require that these requests be excluded from any kind of transparency report that's requested by the data subject, then I think that we need to find another channel, specifically some of the due process channels that law enforcement agencies have that other users of this system wouldn't have, like subpoenas and warrants and court orders and things like that.

I think that's the safest way to do this because otherwise you put a contracted party or a disclosing entity or whatever we're calling it in the middle of trying to satisfy this policy but also trying to respect the rights of the data subject to be aware of these types of things. I think that a due process mechanism provides the best cover for that.

I don't know if we're referencing that work that Chris Lewis-Evans and I had already done or if this is what it has become. I'm not sure. I've lost a handle on that. But I thought we beat this to death already a couple weeks back.

JANIS KARKLINS: Let me maybe ask Caitlin how we arrived at this text, since James raised the issue. Caitlin?

Or Marika?

MARIKA KONINGS: I can try to speak to that, as I think I provided edits. As I said before, James and Chris – I don't know if some others were involved … Indeed, there was a small call that I think tried to draw up some language. Then that was extensively discussed, I think, on one of our previous calls. But I think then that the group came to the conclusion that it was actually very difficult to finalize that language, as the specific requirements would depend on who eventually would be the authorization provider.

So I think we, at that point, left that as an item in which the group said we need to discuss this further. The language you basically see here is just a recognition that … Because, again, from that conversation, it seemed that there was a recognition that, in certain cases, there might be a need for confidentiality. If I recall the original language well, I think the suggestion was that that would be a dialogue between the law enforcement agency requesting that confidentiality and the controller or whoever would be authorization provider making a decision on that based on the information received. But, as said, the group felt it couldn't go any further without that information, so that is what this language is trying to convey: that there was a recognition that it needs to be addressed but that the kind of final requirements around that could only be determined once the authorization provider would be known.

I know the group now has removed that first sentence, which may make it indeed less tangible (what this means), so the group may want to consider reinstating that and really seeing this basically as a placeholder, that it should come back to, once it has agreed on

who the authorization provider is, then determining what kind of requirements or guidelines or whatever the group feels is appropriate should be written in here in relation to the confidentiality of disclosure requests.

I hope that's helpful.

JANIS KARKLINS: I'm not sure, Marika, honestly. As I mentioned, we have two alternates, basically, that we're looking at. Either disclosure would be made by the keeper of a central gateway, or it will be done by one of the 2,000+ registries/registrars. But, in essence, each decision on disclosure would made following this policy by an individual or by machine. So I don't see any difference in terms of how the decision should be made. I'm just simply trying to understand what fix we could make here.

Let me take Greg and then Alan, in that order.

GREG AARON: Hi. There's a question that's going to come out of the Legal Sub-Team about how to balance the rights of the requester versus the data subject and whether the identities of those requesters should be disclosed. That's more specifically about third-party requesters who are not law enforcement. But we may get some more advice in this area that'll inform this later. Thanks.

JANIS KARKLINS: Thank you. Alan G?

ALAN GREENBERG: Thank you very much. I'll note that, under authorization/authentication, we have identity credentials and authorization credentials. In response to James and others to how does the contracted party or how does the entity releasing the information to know whether confidentiality is required in this case or not, law enforcement, for instance, could well use two different authorization credentials, one where, in obtaining the credential, they're certifying that confidentiality is required in this case. For other requests, they could use their other authorization credential which says this is a routine investigation, it's public, and confidentiality is not required.

So we will have a mechanism of flagging the different types of applications, just like we will have – I think the example we gave is that Microsoft might be doing intellectual property protection or might be doing a cybersecurity investigation, and they would use different authorization credentials in each of those cases. So I think we already have the mechanism for implementing this kind of thing. Thank you.

JANIS KARKLINS: Thank you. James, you're next.

JAMES BLADEL: Just responding to Alan, one of the things that Chris and I discussed was the difference between proactively notifying a data subject, "Hey, your information was just requested by law enforcement." I don't think that's what we're discussing here. I

think that we were more concerned – at least I was more concerned – about the notion that some sorts of request need to be excluded, redacted, or omitted from any kind of a transparency report that a data subject might request. I think that – I'm probably blending some different principles from different privacy regulations – they have a right to know if they specifically ask a data controller, "How are you using my data and who are you sharing it with?" If we say, "Can't tell you," we're going to need something a little bit better than a piece of paper from ICANN to get out of trouble on that one. So I think that's where we were circling the landing with the smaller team.

So I'd encourage us to go back and look at that distinction before we just say, "Hey, this sometimes isn't necessary." I'm agreeing with you. Sometimes it's necessary, but, when it is necessary, I think we need to mindful that it probably doesn't belong here and it needs to go to a different channel. Thanks.

JANIS KARKLINS: If the only concern is transparency, then I see a very easy fix. You simply say that a so-and-so number of requests from law enforcement were treated in a confidential manner. That's it. You transparently say that 100 requests have been received by law enforcement without informing the data subjects, and the reason is confidentiality of the investigation.

I have further two, and then probably we need to see how to proceed further. I have Matthew and then I have Alan Greenberg. If I may ask Greg to lower their hands if they're old ones. Matthew, please?

MATTHEW: Hi. I just wanted to add – this goes to your point, Janis, about trying to understand if we can have a unified statement that applies here to both centralized and centralized decision-making – that I think the important thing to remember, and why I believe we flagged that this was something we needed to pause until we knew who was making the disclosure decision, is that the assumption, at least that the Strawberry Team are making under the centralized disclosure model, is that, in order to fully shift that liability and make sure that contracted parties have no oversight or information about the requests that are being made, we're supposed be completely blind to those requests. So I think the challenge that we identified with the centralized response is, how do you communicate that a request needs to remain confidential if the assumption is that the contracted parties are completely blind to those requests under the centralized model. So I think that's the challenge we are identifying and why it matters who it is that's making the disclosure decision here in determining how we move forward with the confidentiality process. Thanks.

JANIS KARKLINS: Thank you. Now I see the point. Thank you, Matthew, as usual. Alan Greenberg?

ALAN GREENBERG: Sorry. I was muted again. I just wanted to note that, if we do manage to come up with some sort of automated release of information in some selected circumstances, requests from law

enforcements, specifically ones that are related to an urgent investigation, may well be among those that we want to have automated. So that's a good reason for making sure it can be done within the system as opposed to reverting to a manual method outside of the SSAD. Thank you.

JANIS KARKLINS: Okay. What I would suggest is that, on H, maybe we still need to ask James and Chris and staff to do a little of back and forth to fine-tune this proposal, and we would bring it to the initial report, clearly identifying that we need to look at it further.

James, you do not want to do that?

JAMES BLADEL: Well, would you like an honest question? I mean, it's Christmas.

JANIS KARKLINS: I haven't said the deadline or the target date.

JAMES BLADEL: Fair point.

JANIS KARKLINS: Next year.

JAMES BLADEL: I just wanted to ask that maybe staff can help us by pulling up the last bit of text that Chris and I presented to the team. I think we should start there. I think we've strayed away from where we had some agreement. If we can go back there and see if we went on course or can we still salvage that, that would be a good starting point. Thanks.

JANIS KARKLINS: Okay. Then let me reformulate my proposal. Staff would, based on our conversation and initial, proposal that you made, together with Chris would see what fix to Sub-Point H we could do. They would run that new fix with you, James and Chris, at the first place and then would share with the rest of the time in the next version of the initial report. So this would be on H.

On I, apart from that it may be moved somewhere else, the essence of point, the substance of Point 1 – is it something we could stabilize?

I see no requests, so we will stabilize I as it is now on the screen, and we will see whether this particular point would need to be moved to another building block, or, in the short report, this will be policy recommendations. I think this is what Brian has suggested. Good.

So then we can go to the next item, and that is purpose, to see whether the suggested item, Building Block B on purpose, the one we could agree on. I assume – yeah. The text is on the screen now. It reads, "As identified in Building Block A (Criteria and content of the request), each request must include information

about legal rights about the requesters specific to the request and/or specific rationale and/or justification for the request – e.g., what is the basis or reason for the request, why it is necessary for the requester to ask for this data. The EPDP team expects that, over time, the entity responsible for receiving requests will be able to identify certain patterns that could result in the development of the preset list of rationales and justifications that the requester can select from while always maintaining the option for the requester to provide his information in free form." So that is the proposal by staff leadership team which resulted in some conversation of the team on the previous occasions.

Marika, you start and then Franck and then Alan Woods. Marika?

MARIKA KONINGS: Thanks, Janis. I just wanted to flag as well that, in the document itself, in the comment that you see on the right-hand side, I think there's some feedback that different groups provided when we originally put this proposal forward. But, to give little bit more context, maybe indeed this [dates] back. I think staff has flagged this a couple times. We struggled with the use of the term "purposes." Immediately everyone thinks back to the purposes we defined in Phase 1 and the status that it has within the context of data protection and registration and specifically the GDPR, while, in the context of third-party access to the data, it seems to be much more about the legitimate interest or the rationale that is to be provided to justify the disclosure of that data. Again, from our minds, where we're confusing ourselves with referring to the purpose (capital P), I think what we've tried to do I the initial report is to move away from that and make clear that what the

requirement here really is about the third party making a request, stating what information – that's something already defined in the other building block of criteria and content of the request – and what each request must include with regards to information about the legal rights, as well as the rationale for the disclosure.

Again, I think, similar what we suggested in the user purposes, in this area, it may also become clear over time that there are set standards or very set rationales that are requested over and over again, which could result in having your SSAD request for disclosure form having a dropdown menu that prepopulate some of those rationales that whoever is managing the system sees over and over again to facilitate that process while never taking away the option of having that freeform option, where someone explains their rationale and legal basis for the disclosure of that information.

So that is a way in which we've tried to overcome that hurdle of the discussion of conflating, I think, what we did in Phase 1 on purposes to what seems to be necessary here. Maybe the difficulty [is] in having that preset list at this point in time but it might be something that would develop once SSAD as in place and whoever manages it has experiences with it.

There is, of course, a second part to that. I think that is a question we did flag in the e-mail when we send this out, which I think is everybody's favorite topic: Purpose 2. You may recall that in, I think, the previous L.A. meeting, everyone said, "We're not sure yet whether we need, but we're not sure either that we did need it. So we're parking for it." So the question we did flag is, is everyone still of the view that it's not clear yet whether it's needed or not?

And, as such, we're not saying anything about it at this stage in the initial report? Is that something where some language needs to be put in, or does this group believe there is further clarity on that topic? I know that's a very big one, so that's maybe one you want to think over over the break. It is one we currently haven't specifically addressed, but the group will probably need to take a decision on whether it is something or not to flag or include in some shape of form in the initial report.

JANIS KARKLINS: Thank you, Marika, for this clarification. Now I have a long list already. Franck, Alan, Milton, and Mark Sv, in that order.

FRANCK JOURNOUD: Thank you, Janis. I hesitate to rehash what we have said before by e-mail or on this call, but, from IPC's perspective at least, providing a fair amount of clarity about purposes is important for several reasons. One is that it provides notice and a sense of fairness to the registrant that data could be accessed and could be accessed for certain purposes. Two, I think it clarifies, as I said earlier, for us the issue of user groups. The purposes are tied. Having clarity as potential requesters of whether a certain purpose or some set of purposes are legitimate or not is important.

That's not to say – I appreciate, in the staff proposed the language, the idea that we don't necessarily won't to bind ourselves and say, "This is the list. There are going to be no other purposes, and they have to be worded this way." With experience, the participants in the SSAD system, which clearly are the

authorization providers, may see these purposes we hadn't thought about, etc.. But the fact that we at this stage believe we can identify certain purposes as being legitimate and in need of being [inaudible] the SSAD policy is a really important point to the IPC.

JANIS KARKLINS: Okay. You're suggesting that we need a list, probably a non-exhaustive list [inaudible]. Maybe someone will bring something new and we will learn by doing. So you're arguing on the non-exhaustive list of purposes. That's my understanding. Right?

FRANCK JOURNOUD: Yes, sir.

JANIS KARKLINS: Okay, thank you. Alan, are you in agreement?

ALAN WOODS: No, surprisingly. But that's not what my point was about. You just caught me off guard and I was blunt. But what I will say is I think we need to be very, very, very careful again, especially based on the legal advices we've received from Byrd & Byrd to date. What we're talking about in that last sentence – specifically, let me talk about looking at this from, say, a balancing test point of view – is an Article 22. We're profiling here. We have been warned against profiling because they [inaudible], according to the legal advices that we have received. So we have to be exceptionally careful on

that one because profiling leads to all sorts of issues that we don't want to put down on paper, to be perfectly honest.

I also want to point out the fact that I'm okay with the concept that – I'm happier with the concept – the entity responsible for receiving requests that will make the decision. I think that is exceptionally important, especially in light of what we've just gotten from the Belgian DPA, which has all – [inaudible] people who disagree with me but who put the kibosh on the concept that liability can be removed from the contracted party because, in this instance, it's very important to point out that the contracted party's liability will be very much at stake here, especially if that is the entity responsible for making the decision unilaterally for all parties involved in the data processing sphere.

So I just want to make sure that we understand what we already had on file as legal advices and that we are taking that into account. We should be very, very, very careful not to put something like this down on paper and putting it out there for everybody to see because it looks like we're ignoring our own legal advices on this.

Now, to [inaudible], there are other instances where 61F is not the actual legal basis. Then that is absolutely one of those instances that we've always said there's a potential for automation. But not here. [That's the question.] Thank you.

JANIS KARKLINS: Thank you, Alan. Milton is next.

MILTON MUELLER: I think Marika set us on the right track when she introduced a clear distinction between the purposes of WHOIS and of ICANN and having WHOIS and these kinds of classifications of requests. So these are not purposes in the capital P sense that we debated for so long. These are particular rationales that the requester is making. So I really think Franck's comments concern me a bit because they seem to be dragging us back to the purpose debate when in fact this is a separate issue. It's an almost an operational issue. What do requesters say to the SSAD operator? How do they classify or characterize their requests, and how do they justify them?

So we are very okay with the first half of this paragraph. We're a little bit uncomfortable with the second half. I don't know about everybody in my stakeholder group, but, in some sense, this is unobjectionable in that, yes, if you get 6,000 requests saying, "I'm a trademark owner, and this domain is in violation or infringement of my trademark rights," then having a little pulldown menu that says that is okay.

What we are extremely worried about is the idea that, if you mark that box, you are automatically assumed to be correct and there would be not actual evaluation. So, when you start linking these kinds of preset rationales with talk of automation, that's when we get nervous. We would reject that kind of an option. So I hope everybody understands that distinction.

Let me speak again to why we do not need any kind of a preset list defined by policy because, again, then you're saying that any rationale that doesn't conform to that list is excluded. We're going to get into an unending series of possible categorizations. We're

going to have to end up saying it's non-exhaustive. Then people who don't have their little favorite cause on the list are going to get worried. We really don't need to go down that road. Requesters make their case. They put whatever justification they can. Some of those justifications may be very routine and cut and dry. That's fine. But let's not confuse that with any need for listed purpose.

In fact, I would actually propose to delete the term "purposes" from the title of [the link] on B and all it justifications. Thank you.

JANIS KARKLINS: Thank you, Milton. Next is Mark Sv, followed by Amr and Margie.

MARK SVANCAREK: Thanks. Milton is right when he says this is an operational issue. That's really why I'm concerned about it: remember, the people who are doing the implementation will not have been as steeped in this as we have been. They will not be as expert on GDPR. They will not know the motivations of us as we create the language. So there are some cases where creating more specific language, even though it's maddening, will actually benefit us down the road.

So I do like, from an operational sense, to have some sort of enumerated list, where, later in implementation, we're not arguing about what sort of things are available or what specific language needs to be used. If the specific language is in fact incorporated in the enumerated list, I think that could be beneficial. Of course, it's not exhaustive, but in this case, I think that's okay because you just have a checkbox that says Other. Then you have the freeform

justification. That freeform justification is now subject to all the concerns that I just mentioned, but at least that would be a smaller subset.

Regarding profiling, I'm a little confused by Alan Woods' concern that this is profiling. I guess it's profiling of the requester. I wasn't aware that that was actually of concern to GDPR. I don't see how this would be a profiling of the data subject. But maybe that's because there's some vagueness in the wording. So the intent of this, as far as I know, was to categorize: these type of requesters make these types of request. So, if it's being perceived that this is a way of profiling the data subject, then, yeah, we should change this and find a way to make that list ambiguous.

Of course, not surprisingly, I didn't interpret the Belgian DPA as putting the kibosh on anything but really just lecturing us that, however you allocate the various types of processing, whoever does the processing is accountable for it, which I didn't think was controversial but doesn't actually help us how a joint controller agreement is going to work. Thank you.

JANIS KARKLINS: Thank you. Amr is next, followed by Margie and then Franck.

AMR ELSADR: Thanks, Janis. I completely agree with everything Milton just said. I'm very concerned, especially in the context of an automated process to the extent that automation is possible, that a list of purposes presented to a requester will effectively give the

requesters a cheat sheet to make sure that their requests for disclosure are successful.

I think also that the proposal Milton said of renaming this building block to justifications is a very valid point. The purposes we're discussing should be restricted to the purposes of disclosure on the disclosing entity's part. They're not purposes by third parties. As Milton said, those are justifications for disclosure, and they have to be consistent with the controller or the disclosing entity's purposes.

So it seems more reasonable to me that a requester should, in their own words – they don't need to be legislative experts on GDPR – explain why they believe they have a valid reason or justification for disclosure. Then, if those are consistent with the legal purposes on the controller or the disclosing entity's part, then, sure, that should be done.

In that sense, also we need to very much separate what these justifications are as opposed to the purposes that are communicated to a registrant, as is required. When a registrant agrees to the terms and conditions by registrar or reseller [– the one] registering a domain name – then the purposes by which, again, the disclosing entity might share personal information with a requester. Those need to be included, but those will not include a list of justifications on a requester's part. It's a different list. I don't believe that they should be conflated at all. Thank you.

JANIS KARKLINS: Thank you, Amr. Before going further, may I, Berry, ask you to, after "requester" in the brackets in Building Block B, put "requester justification"? Just to capture [that] this idea that has justification.

Then if I may ask you also to separate this paragraph into two paragraphs, the second starting – yeah. Exactly. So on automation.

With this, now I invite Margie, followed by Stephanie, and then Alan.

MARGIE MILAM: I just want to reiterate points we've made in our e-mails and prior discussions that the BC believes that a predetermined list of purposes is necessary. This is an issue where we dissented from the final report because Purpose 2 did not specify the third-party purposes that we've been talking about: cybersecurity, infringement, and consumer protection. So this is just one of those areas that, if we do not have a specificity in the policy, we're going to have a hard time supporting the entire policy.

I think that, if we can find a way to accommodate the need for specificity here, it will also be supported by GDPR, where GDPR requires that the purposes be disclosed to the data subjects, such as the registrant.

In this case, I disagree with what Amr said about it being a different list. If we're telling the registrant that their data could be used and disclosed to parties interested in protecting their intellectual property or protecting against cybersecurity threats, that list needs to be specified in policy.

I'm not hearing from this group an objection to the concept that cybersecurity is a legitimate purpose for seeking disclosure of the data, so I'm asking that we find a way to include that in the policy because it is so important to, certainly, our stakeholder group.

To follow up on some of the comments that were made up about the memos and liability and profiling, I don't understand Alan Woods' concern about profiling and where it is considered illegal. Profiling is not that different from correlation, and we've been talking about the need to correlate data to identify trends. That's certainly something that SSAC has raised. Greg Aaron has raised it multiple times. I've raised it multiple times. That's not illegal in that context.

The other thing that I think that we need to also talk about – we'll talk about it next year, I guess – related to the liability is that I think we need to approach this from the perspective that we have never said there would be no liability to contracted parties. That is not the goal of this group. The goal here is to minimize liability. I do not see the letter from the DPA as saying that there's no way to minimize liability. All I see is a request for additional information.

So part of what we should do from the policy perspective is think about ways of minimizing risk. We, as the BC, have made suggestions, such as insurance or bonding. We're talking about contract terms, such as indemnification. Those are all things that can minimize liability, and I wouldn't be looking at the letter from the DPA as a eliminating those possibilities.

JANIS KARKLINS: Thank you, Margie, for your comments. Stephanie and Alan G and then I will make a proposal, taking into account time. Stephanie, please?

STEPHANIE PERRIN: Thanks. I would like to express my qualified support for what Amr and Milton have previously said. I'm really worried about the conflation of purpose and these common purposes of certain groups of requesters and the tendency for automation to make associations that become permanent. So I think they've already discussed that.

I also agree with Margie that a list of purposes and the kind of details that we're talking about here somewhere is required under transparency but I'm not sure, again because of the risk of conflation, that it belongs here.

The other thing I'd like to query is – we've argued about this in the past. I'm not questioning that a requester has rights under law to, for instance, protect their trademark. But the legal rights of the requester is a bit misleading. The requester may also be operating under either fiduciary obligation or legal obligation.

An example of that, for instance, in Canada, last time I checked, was that someone changed our child pornography law. There's a positive obligation for ISPs to report if they detect it. That's not their legal right. That would be an obligation under a separate law. There are other kinds of administrative law where the same thing might apply.

So I think this is swaying things towards the legal rights of the requester which are questionable and make us that their rights under GDPR – legal reasons, perhaps? – might be better. Or add in obligations. Thanks.

JANIS KARKLINS: Thank you, Stephanie. Alan G is the last one.

ALAN GREENBERG: Thank you very much. I want to comment on, I guess, Milton's, Amr's, and Stephanie's, saying there's not automatic to data, whether "right" is the right word. We can't release data automatically because something fits a patter. I think we have to acknowledge – I know contracted parties have – that there are going to be large volumes of request that fit in a specific pattern.

Now, the definition of insanity is to do the same thing over again and expect a different answer. If the pattern is followed, and if it is one that has been routinely accepted, then one can assume that information will be related. Now, it's going to be modified by exactly who the requester is. If this is a requester who's following a pattern but has a history of abuse, then, of course, the data may not be released. But, in a typical situation where we don't have red flags associated with the requester or perhaps with the domain being requested that may have to be treated differently, then these things will be automatable. We can't insist that someone spend five minutes musing over a request when it is identical to the thousand that came before and the thousand that came after.

So I think we have to be practical in terms of how we're going to implement this. We may not know what that pattern is today, but history will build up pretty quickly as to what kind of patterns can be handled with some level of automation and what kind cannot and must not. Thank you.

JANIS KARKLINS: Thank you. James, do you insist?

JAME BLADEL: Just very briefly. Alan makes a lot of sense from an operational perspective. Obviously we want to identify common elements and automate as much as possible, but, from a legal perspective, I think that invites folks to try and sandwich questionable requests in between large batches of obvious and very simple requests. I think that that is an incentive that we want to avoid. Thanks.

JANIS KARKLINS: Thank you. Certainly that's true. I think this text needs further reflection in light of the conversation and maybe some tweaking. I would suggest that staff, based on this conversation, would try to analyze and see what could be changed.

In the meantime, maybe somebody could volunteer and draft that list of justifications – let's say, the most common. That will give us maybe an idea of what we're talking about – most likely, that would be the BC, who was arguing that that list is needed – for our next conversation next year, not for Christmas. We would then revisit this conversation during the first call of the next year.

So that would be my proposal for the moment. I see Brian's hand is up.

BRIAN KING: Thanks, Janis. Just to reiterate that specificity and purposes is one of the most important things for our group to be able to sign onto this final report. I want to be clear about that early in the process, just so that the chips are down and it's clear that we need that specificity here.

We have language in this report that I think everyone has agreed to that says that every request needs to be evaluated on its merits. So I don't think I'm sympathetic to the concerns about profiling registrants and things like that. I don't think anybody is suggesting here that, if you state that you have a purpose that's among the list of purposes provided to the registrant, which the law requires, by the way, there's a risk that, just because you state that, anybody thinks you get carte blanche to the data or that your request should be simply approved. We've worked long and hard on lots of safeguards and lots of other requirements that need to go into the request. So I'm really not sympathetic to that concern here when we have all that baked into the policy. Now, the law requires that the purposes are explicit.

As a procedural point, we talked a lot, in the first phase of the EPDP when we were concerned about specificity and purposes, about ICANN's purposes and the registrants' purposes and the contracted parties' purpose in Phase 1. When we got to Phase 2, that's when we would talk about third-party purposes and make those clear. And here we are.

We said the same thing about access as well. I just have to say that, when we get into Phase 2 and then nobody wants to talk about access anymore and we only want to disclosure and now we don't want to talk about purposes anymore but we want to talk about justifications, it doesn't come across well. I don't think we're on the same page. So we need to do what we said we were going to do and list those third-party purposes. Thanks.

JANIS KARKLINS: Thank you. We still need to talk a little bit through next steps. Milton, please be quick.

MILTON MUELLER: Yes. Again, most of what Brian said would be okay if he stopped talking about purposes and started talking about justifications. All of those might be acceptable as justifications for requests for disclosure, but when you're saying their purposes, you are creating a lot of confusion regarding their legal justification and the relationship to other parts of the policy. It does imply that all of these justifications are automatically valid. When you have Alan Greenberg suddenly saying, "Yeah, we're going to have to automate this based on profiling," that's exactly what's kicking up the resistance. So you've threatened a couple of times now that you're not going to support this report. Anything that leads to automation based on simple categorial assertions in a database is not going to get by us. So keep that in mind. Thank you.

JANIS KARKLINS: I don't think that anyone is threatening anyone at this one. We're simply trying to make our points with the things we believe in and we're expecting. This is very good. It is much better to know it now than at the end of the process.

On the screen now – it will stay on the screen for the moment – this a list of purposes or justifications that the BC has put forward earlier. For the moment, we need to think about whether and how and where to capture that text or at least notion.

We have now a little bit of festivities and break ahead of us. We will come back to this conversation during the first meeting of next year. We will continue because this was not [inaudible].

In the meantime, please think about these points and whether there was something you cannot live with or completely object to or if there's anything that is missing that would need to be added, with the understanding that, whatever we do, this is not our conclusive list but there might be something else that was not on the list.

With this, I would suspend conversation on this building block and move to the next agenda item, which is next steps. Here we have the Christmas present made by staff. I will ask Marika to introduce the Christmas present. Marika?

MARIKA KONINGS: Thanks, Janis. I think we'll actually be able to give everyone an early Christmas present because staff has been working on an updated version on the draft initial report, in which we'll basically list in all the building blocks we've discussed over the last couple

of meetings and where text has been stabilized. Or, in cases where it hasn't, we'll, of course, mark that, like some of the topics that have been discussed today. We hope to publish that either later today or tomorrow.

The idea here is that we'll create a new Google Doc link. We've already tried to address as well some of the comments that some of you made where it concerned, at least from our perspective, minor changes or updates. We'll also start flagging which items will need to further considered by the EPDP team in the new year. The hope is that basically the initial report will now come [from] the list or the master document from which to work off.

So our question to you is, once the new link is circulated – we already created a specific wiki page for it, so it should hopefully be easy to find – by the 7th of January, your respective groups will have basically reviewed this document. Basically, we're asking you ask well to not reopen previously closed discussions unless there is new information to consider. If you just want to make your same points, it may not be productive to do that again in the document.

If you have concerns about certain sections or certain language, mark that in the form of a comment. Don't redline the text, please, because that may become confusing. We would really like to encourage that, if you have a concern, at the same time, identify how that concern could be addressed, also, of course, factoring in what others may have said or indicated about certain topics. Put that in the text. We'll use that basically to develop from the 7th of February onwards the running list of topics to be discussed over the meetings that will lead us into the face-to-face meeting.

Of course, if there are minor edits – grammar or style – you can even send those to us directly or, again, flag them in a similar way in the document. Those we can already hopefully resolve before we get to the next meeting.

So that's it. Happy holidays.

JANIS KARKLINS: Thank you, Marika. Thank you for the gift. We were expecting that today or tomorrow.

As I indicated, we would come back to a discussion of purposes during the first meting of next year, which is, I think, scheduled for the 9th of January. And we'll continue from there. Our objective is to come to Los Angeles in order to finalize the report and then publish the report after our face-to-face meeting for public comment.

With this, I would like to thank all of you for active participation in the meeting. I'm wishing you a very, very Merry Christmas and a Happy New Year. This meeting stands adjourned.

[END OF TRANSCRIPTION]