ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Tuesday, 22 October 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/I5ACBw
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 22nd, October, 2019 at 14:00 UTC. In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourself now? Hearing no one, we have listed apologies from Ayden Ferdeline (NCSG), Julf Helsingius (NCSG), and Ashley Heineman of GAC. They have formally assigned Tatiana Tropina, [inaudible], and Laureen Kapin as their alternate for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their line by adding three Zs to the beginning of their name, and at the end in parenthesis, your affiliation, dash, alternate, which means you are 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 chat, apart from private chats, or use any other Zoom room functionality such as raising hands, agreeing, or disagreeing.

As a reminder, the alternate assignment form must be formalized by the way of the Google assignment link. The links 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, please contact 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 circulated on the mailing list and posted on the public Wiki space shortly after the end of the call. With this, I'll turn it back over to our chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Good morning, good evening, everyone. Welcome to the 26th meeting of the team. So let me start my usual question. The agenda that was circulated to the mailing list yesterday, would it be acceptable for us to follow during today's meeting? I see no objections, so we will do so.

The first sub-item on housekeeping issues is proposed outline for EPDP plenary meeting at Montreal. As you know, during the Montreal meeting, we will have 14 meetings and one main session at the main hall which is scheduled for Monday from 10:30 to noon. I don't know whether we can put up on the screen the proposed outline of the session. This is what you see now on the screen with the order of interventions, prior giving opportunity to community ask questions will provide comment. So, we would start, as you see, with welcome and introduction of chair of GNSO. Then I would explain, in essence, what we're doing. Then, Strawberry Team would outline the work that they do and the state of their activities. Then I would conclude by presenting expected timeline and engagement with community prior to opening to Q&A.

So, this is the proposal which has been also circulated to GNSO and GAC leadership and they are in agreement with that type of approach. So, that's where we are. Any questions? James?

JAMES BLADEL: Thanks. Yes. I'm just catching up with Marika in the chat that this is for the plenary session but I just noted that ten minutes with the Strawberry Team is really not even enough to get in introductions and get everyone's name out, so hopefully, we can find a little bit more time with them somewhere later in the week. Thanks.

JANIS KARKLINS: No, no, no. I'm talking about the plenary session that we have where we will be organizing together with GNSO and the GAC. So, it's not the team meeting as such. It is simply the main meeting room where our work for the first time will be presented to the community as a whole. So, we will be talking with the staff, or I will be talking with the staff and Rafik, next Monday how to better schedule our activities in Montreal as a team and we will propose outline of our meeting during the Tuesdays call that we will be have next week. Next week, the only call we will have is Tuesday.

As I mentioned, we will meet all day Saturday. That is the one meeting. Then, we will meet for one-and-a-half hours on Sunday afternoon. Then we will meet for one-and-a-half hours on Monday afternoon. Then we will meet on Thursday for one-and-a-half hours on Thursday afternoon. So these would be four team meetings during the Montreal. Marika?

MARIKA KONINGS: Yeah. Thanks, Janis. One thing I wanted to note is that on the Q&A session, staff [inaudible] with the leadership team to put in some potential questions that could be put up for discussion and especially looking at where could the group potentially get constructive and new ideas in relation to some of the questions and maybe struggling with. But again, these are just example questions and I think we would be really looking towards the EPDP team to get some suggestions or ideas on what would be good questions to discuss in a plenary setting. I think we want to avoid any kind of questions where we already know the different types of answers because they have been discussed in the EPDP team. But maybe there are certain questions or areas where sharing that with a broader group or asking very targeted questions may result in some input that is new or where the group hasn't thought about or some innovative approaches. So, I think that is something we're really looking to the EPDP team for suggestions. We can of course share this again on the list on the call for proposed questions and those can then be shared and further refined as needed.

JANIS KARKLINS: Thank you, Marika. So, maybe Marika, you can type in the chat the schedule of our activities during the Montreal meeting, so everyone has it. So, with this, I understand that we clarified what this session is about, this cross-community session requested by the GAC and GNSO and we'll be prepared to interact with community as necessary.

So, with this, I would like to go to next item of our agenda and that is questions to ICANN Org. Here, if you recall – Margie, you have your hand up.

MARGIE MILAM: Yes, thank you, Janis. Sorry, I didn't take up my hand fast enough. About the Montreal schedule, will we be talking about the building blocks? I'm just trying to understand where we're going to be in the building blocks and what's expected the conversation to be surrounding.

JANIS KARKLINS: Yes, we will be talking about building blocks, hoping that we would manage to finalize all of them. That will be very challenging, but I'm still hopeful.

MARGIE MILAM: So, will we have a document that is shared with the community or is it just whatever version is on our—

JANIS KARKLINS: Sorry. You're talking about the community session, cross-community session, or you're talking about team meeting?

MARGIE MILAM: I'm sorry. I'm talking about the cross-community session.

JANIS KARKLINS: No. I will simply outline the general approach, what we're working on. What are those building blocks? In a few words, what's their reason, what they entail. That's more or less … And actually, you can see a few days ago there was a GNSO webinar where I made the presentation and that presentation will be the basis for presentation in Montreal. In Montreal, maybe it will be slightly more detailed with more elements on each building block. But not much more detail.

MARGIE MILAM: Okay, thank you.

JANIS KARKLINS: Sure. So, the next sub-item, questions to ICANN Org. If you recall, we started working on formulation of questions that we could ask ICANN Org in relation to different aspects, systemic aspects, of SSID, whether they would be maintaining their own RDS replica database, whether they would be ready, yes or no, make determination of the [inaudible] of request, whether they would be assuming responsibility for decisions, each scenario that that would be assigned to them and so on.

So, those questions were informally shared with ICANN Org but then we decided to send a letter to the board which was done, and we're expecting an answer from the board, mostly likely after the Board Workshop in Montreal. But I still believe that some of the elements that we wanted to ask ICANN Org could be asked and my question to you would be whether you would not object me sending an email and asking ICANN Org to provide input to those – answers to those questions for my own knowledge and better understanding of position of ICANN. Then, of course, ICANN Org. Then, of course, that information will be shared with the team for the benefit of the team. So, that's my question. I'm really willing to send those questions in and see what type of answer ICANN Org would provide us. And without prejudice what board will answer us. So, these are two different things. Any objections? Marc Anderson?

MARC ANDERSON: Yeah. I don't even remember what those questions are anymore. I'm sorry. Are they available that you could throw them up on the screen maybe?

JANIS KARKLINS: Yeah. I don't know whether we can put them on the screen or we can share in the chat. Let me see. I outlined a few of them. Does ICANN have a clear preference on whether or not it will field these requests for non-public data, maintain its own RDS replica database, make determination on the eligibility of the requests, assume responsibility for these decisions in a scenario where ICANN does not hold the data directly and must require contracting party to respond to requestor, given the contracted party disputes [inaudible]? So, those are four questions that we formulated and informally shared with the ICANN Org liaisons and they have been informally submitted to ICANN Org.

Look, we can … Caitlin, could you share it on the chat, maybe, for the sake of the team? So, do you have any concerns with those, Marc?

MARC ANDERSON: Thanks, Janis. I guess I don't have any concerns after rereading that list. I guess my only question is could we improve on them? I think those were pretty rough questions. But to answer your direct question, no, I'm not going to object to that.

JANIS KARKLINS: I'm not planning to send it on behalf of the team. I am planning to send them as chair of the team for my own knowledge. But of course I'm happy to share answers with the team for information. Whatever will come out, I think that would inform our discussion. So, that would be my approach. Georgios?

GEORGIOS TSELENTIS: Yes, Janis. I think it is useful for the group to have, if not clear answers, at least some possible answers, even with options. So, I would urge you, if you forward those questions to ask also ICANN to be as complete as possible to the answers, and if they cannot answer directly a question, they can even give possible options without preference. I mean, if this helps getting some clarity, because I believe those questions are giving us some more information about what the possible implementation of those policies would be and what the role of ICANN and those policies might be. Thank you.

JANIS KARKLINS: Thank you, Georgios. Provided that we entrust ICANN to do something. So, without prejudice, the outcome of our conversation. Of course. Brian?

BRIAN KING: Hey, Janis. Thanks. This is Brian. I would just add that it seems that these questions to ICANN Org are closely related to the question that we posed to the board and just knowing how ICANN works, Org will need to do what the Board tells them to do. I wonder if we should ask these questions in a related way to the Board in addition to Org. Thanks.

JANIS KARKLINS: Yeah. I don't know. I'm not … I don't think we should overcomplicate it. The most important thing is to keep communication floating, and even the answer is no, the negative answer also [is answer] if answer is yes. But that's even better answer and so on. And if we will start negotiating questions, that may take time, and we're talking about a quick return, potential quick return, by Montreal meeting. And certainly they will be discussed in conjunction because I doubt that board members will write a reply to our letter by themselves. That will be ICANN staff supporting the Board who will be making a draft and then Board will be editing proposed text.

I see that there is no objection. I will do so. And I suggested also … Georgios I will ask maybe to provide options if a clear-cut answer at this stage is not possible. And I will send it on my behalf under my responsibility in my capacity as the chair and it will be clearly stated that it is not a team letter, it is chair's letter. Okay, thanks. Shall we now take visuals where we are, status of building blocks?

UNIDENTIFIED FEMALE: Terri, if you can stop sharing your screen, I'll share the overview. Thanks.

JANIS KARKLINS: So, regrettably, we're exactly in the same place we were last meeting, before last meeting. I would like to use this opportunity, not really being a professor at school but simply encouraging team members to maybe make an extra effort in order to provide input if they volunteered to do so. It is essential for me as a chair to know that if somebody volunteers to do something, that this is done, and if it's not done for one or another reason, that there is an [interim] information saying these are the reasons why the task could not be completed but it will be done by … And then the new date.

Why I'm saying this, because I really rely on input of team members as penholders on different topics, and if I know that there are no volunteers – for instance, on building block M, at least not for the moment, then I ask staff to make a first draft. Not optimal but at least this is the way how we can progress because it's much easier to edit text and then discuss on the basis of existing proposal, rather than do editing on the fly. So, therefore, my appeal to you, I know it is hard, I know we are tired. Christmas is coming and it would be really good to have Christmas with initial report behind us. Again, my appeal to do homework, to come to the meetings with an open mind and with a constructive approach that we can progress.

Also, you will see in the next agenda item that I propose to use colors because last meeting we started to renegotiate things that we had already agreed on, at least majority opinion wasn't in that direction, so therefore those texts that will appear on the screen in green should not be questioned unless there is a complete misunderstanding and mistake. Otherwise, I would encourage not to discuss anymore those texts that are in green. Again, that will help us to progress quicker.

So, I see a number of hands. Marika, is your hand up or is that an old hand?

MARIKA KONINGS: No, it's a new hand, and thank you very much, Janis. I just wanted to flag that we've also added new building blocks that we've discussed in the context of other building blocks in relation to audit requirements and logging requirements, where first drafts have been produced and there was also, of course, open fora for input from the group.

One thing I may want to suggest, following Janis's introduction here – and it's something we haven't discussed yet on the leadership team but it's maybe something where the group may want to think about as well, because one of the things we've been challenged with is that input is provided very close to the call which doesn't give anyone the opportunity to kind of review that input which results in a lot of thinking out loud during the call or seeing input for the first time around and I'm just wondering whether for the Montreal meeting we should think about having a date at which we will freeze all the documents or all groups are requested to have their input in on all the building blocks by X date, at which point we'll freeze them and use that version and the input that is received by that date to prepare for the sessions in Montreal which could be in the form of modified versions that aim to address the comments received or specifically outlining what the open issues are. But that may be a way of having everyone work towards a very specific deadline, of providing input and having a kind of frozen state which will be the basis of discussion instead of moving target which I think has caused some issues for us in some of the recent calls.

JANIS KARKLINS: Thank you, Marika. Alex Deacon?

ALEX DEACON: Hi. Thanks, Janis. This is Alex. So, I just wanted to say I've returned from two unplanned weeks away from the EPDP and other things, so I've been catching up as quick as possible and I plan to submit IPC comments on the accreditation building block by the end of the day today. I know it was due last Friday but hopefully the input will add value and be helpful. Again, apologies for missing that deadline. Thanks.

JANIS KARKLINS: Yeah. Thank you, Alex. It will be very useful because Thursday meeting will be on accreditation. Marc Anderson?

MARC ANDERSON: Similarly to Alex, noting that Hadia and I had an action item to work on one of the bullets under accreditation. We're still working on that. We're making good progress and hopefully we'll have something to submit very soon.

JANIS KARKLINS: Thank you. So, on accreditation, please be aware that based on our discussion last time, staff did very serious rewriting of accreditation building block and therefore we will put out the new version soon after this call. So, I have been corrected it was not serious rewriting, but more serious reorganization of the text. Nevertheless, it will look different. Just for your information.

So, with this understanding and my appeal, I would like now to move to the agenda item number four, which is acceptable use policy, if we can get text on the screen.

So, acceptable use policy. That is building block D and H, one from requestor side and one from information provider side. So, as you see A and B are in green, I think we have discussed it and stabilized this with auditing. As you will see, there will be a new building block, auditing, and every auditing aspect will be addressed in more details and this here only will be a simple reference that these thing will be subject to audit in general.

So, we are now on C, where some additional discussion was needed, so proposal by the staff is that requestor must provide a) representation regarding the intent use of requested data b) representation that requestor will not process data in a manner that is incompatible with the purpose for which the data was requested and this presentation will be subject to auditing with understanding that this will be described in auditing building block. Any issue with this C? Marika?

MARIKA KONINGS: Thanks, Janis. Not an issue, but just to flag this was indeed language that staff put in following the last call during which this building block was discussed but there was also an action item for Margie and Amr to work on updated language for this section. I know that they had been discussing and, again, I don't know if the staff language or proposal was helpful here but it may be helpful to hear from them whether they expect to make further updates or suggestions for this particular section or whether the version as is currently on the screen is what the group is considering for approval.

JANIS KARKLINS: Thank you, Marika. Amr?

AMR ELSADR: Thanks, Janis, and thanks, Marika. Well, I see Margie has got her hand up. If she'd like to go, I'm happy to yield the mic to her.

JANIS KARKLINS: Go ahead, Margie. Thanks.

MARGIE MILAM: Thank you, Amr. Yeah. We did talk about it. I think there's one area where we did reach agreement. We did not reach agreement on the language, not process in a manner that is incompatible with the purpose. I think Amr and I view the language in GDPR differently. But I think the area where we did reach agreement was that we should be able to allow for the requestor to submit more than one purpose. In the scenario where I was worried about where it could be, say, trademark infringement. It could also be cybersecurity if it's a domain name that's going to be used for phishing and has a trademark in it, that we just want to make sure that the request can include the selection of more than one purpose, as long as it's applicable. It's not meant to be something that you'd be clicking off anything for the sake of over … To cover all your bases. But if you have a reason to believe that more than one purpose would apply, you would be able to do so.

So, I think that was the only area where we had agreement. I think Amr is still concerned about the language I think probably that you see in the proposal in C.

JANIS KARKLINS: Okay. Thank you. Amr?

AMR ELSADR: Thanks, Janis, and thanks, Margie. Yeah. Just to go ahead and confirm what Margie said, I think we both do agree that requestors need to be as thorough as they can in their disclosure requests, so if there are multiple purposes for which they might need to process the personal information, then they should be allowed to include these different purposes. And some of the examples Margie gave are pretty much what we had in mind.

In terms of next steps, practically speaking, I think where Margie and I are at right now is that we are going to probably just type up a proposed revision of C based on the bit that we do agree on, and then provide rationales. Just sort of like a summary of our discussions and why we each have differing opinions on the rest of what's in subsection C here, and hopefully get that to the rest of the EPDP team by the end of this week. Thank you.

JANIS KARKLINS: Thank you. Can we think of [inaudible] of agreeing now? Look, staff was looking up and was using the language from GDPR, so I think we can find the fix for the agreement that has been reached is that in the bullet 2i, we could use representation that the requestor will not process the data in the manner that is incompatible with stated purposes for which the data was requested. Stated purpose is, which is in plural which alludes that there might be several – or purposes without stated, where the idea is we put purposes in plural and things are clear. Alan, are you in agreement?

ALAN WOODS: Thanks, Janis. Not really, unfortunately. I think that's kind of missing the niche point that has been put on this, and that is that when you're disclosing this data, the disclosee, they may be a controller in their own right. However, in the instance of that disclosure, they are not the controller. They are a disclosee. What we're suggesting here is to give them the right to change the purposes as were stated to the actual controller at the time. That is not incompatible with the original purpose. And that unfortunately is not how … Even though it is the wording of the GDPR, it is how it relates to the primary controller, not the disclosee.

So, I'm kind of echoing and mirroring what Amr would be saying on this, that I would have difficulty in accepting that the disclosee would then be able to go and subtly change the purpose for which they are using that data and I think it's probably, as a safeguard, best for us to insist that if the disclosee is going to be stating specific purposes, that is the purpose to which they must then use that data.

If they have a separate distinct purpose but maybe has arisen out of review of that data, well then that probably would change the very basis for the request anyway, and therefore it should be not necessarily a new request but it certainly should be an update or addition to the family of that particular request. I think we have to be very clear that it is not clear cut that they can change subtly those purposes, just because they have that data in hand. I think that we're missing … It's not the purposes or not the problem is the incompatible word or the compatible word in that. That is probably where the fudging, unfortunately, begins in my mind and I think there is definitely a bit of more discussion will probably be needed on that. But that would be my view. Thank you.

JANIS KARKLINS: Okay. Thank you. Let me take Mark SV before.

MARK SVANCAREK: Thanks, Janis. I would just like to call back to Alan. Could you explain that a little bit more? I think I know what you're saying. What I didn't understand was the specific criticism of the language that you said was already in the law and the distinction between the various controllers. I didn't follow that. Could you clarify that for me? Thanks. Sorry.

JANIS KARKLINS: Alan, you are on the spot now.

ALAN WOODS: No, that's quite all right. And if you indulge me for a second or two, absolutely no problem. I think the easiest way to perceive this is from the point of view of our friend, the data subject. The data subject is going to be told as a very important aspect of any update that we make or any creation of the SSID, that your data may be given to people who meet a specific standard and that specific standard is they have a legal basis and [specificity] for purposes as stated. We cannot say to them that it will be purposes as states or any purpose that they might deem would be compatible with that.

Again … And this brings down the fact that there are two different types of controllers and the primary controller is the controller who has that distinct link to that registrant, to the data subject, and that data subject now understands that there may be an instance where their data, when it is looked at by that controller may be disclosed for stated reasons. They do not agree and they cannot agree because it's just far too wide and broad a field that that then, that disclosee, might then decide whether or not they think that there is a purpose for which is compatible because it's diluting that initial notice to that data subject. They can't foresee what potential it is.

Also, another problem is that they do not know who this disclosee is. They might not even be aware who this disclosee is until they make a request for a data access request.

So, again, the dilution here is that we need to ensure that the data subject understands for what purposes and then that controller must be able to answer for what purpose specifically that data was disclosed. They can't just say "or any other purposes" that they might have felt was compatible with that. I probably mauled that a little bit in the run of it but I'm happy to discuss that with both Margie and Amr and I think give a bit more detail on that. Thank you.

JANIS KARKLINS: Thank you. Let me take now Brian King.

BRIAN KING: Thanks, Janis. If I could suggest perhaps a slightly different approach that I think might make this a little more easier and track a little better to GDPR.

If you look at Article 5, what really it requires is that the data is not further processed in a manner incompatible with the purposes for which the data was requested from the data subject. Sorry, not requested. I'm reading on the screen here. Collected from the data subject. So, this might do the trick if we rephrase this along those terms, make representations that the requestor won't process the data in a manner incompatible with the purposes for which the data was collected. That I think is helpful because, one, it tracks better to GDPR. But two, it gets us out of the world of getting too much into what this unknown requestor is doing with the data.

I think, if I were to council ICANN on this, I would say stay away from getting yourself into what the requestor does with the data after they have it. ICANN's responsibility is to make sure that the requestor has made the proper representations about what they'll do with it, and if they lie to you or if they change their mind or if they break the law, that's between them and the data subject and the DPAs. And really all ICANN is in a practical position to do is to collect the appropriate representations to cover its own processing of disclosure to that third party.

So, I'd caution us not to go too far down that road, and I think doing that and keeping the request here is that the requestor agrees not to process the data incompatible with the purposes for which it was collected will do that for us. Thanks.

JANIS KARKLINS: Okay. Thank you. Amr, I'm holding you. Let me see if we can … I have a feeling that there is need for further refinement. Volker, please, go ahead. Then Amr and then Alan in that order. Volker?

VOLKER GREIMANN: Thank you, Janis. I like the suggestion that Brian made but for one issue. I think we are on the right path there but that doesn't solve the problem that we originally wanted to address when we proposed this. Ultimately, we want to prevent the old switch-a-roo where someone comes and says, "I want to have this data because someone is doing something very bad," but actually they do want the data for something else that they do not want to disclose and therefore they are abusing their access. I think that is what we are trying to address here.

While the change that Brian proposed is I think a very good change and should be in there, I think we still need to have a safeguarded place that also takes care of this other problem. Thank you.

JANIS KARKLINS: Thank you. Amr?

AMR ELSADR: Thanks, Janis. I completely agree with everything Alan Woods said earlier and had very little to add to it, but then Brian kind of jumped into the point that I wanted to make. Again, I think my understanding of Article 51b is a little different from others.

Like Alan pointed out, a requestor can become a controller after the fact, after disclosure has been granted. But during the disclosure process, they're still not controllers. They're still just requesting that the data be provided.

Now, to me, Article 51b points to the original purposes – legitimate purposes – for which the data was collected by, let's say, controller one, our primary controller. The real issue we're trying to solve with this subpoint here is whether the requestor has to update the request or submit an additional request for additional purposes, whether incompatible or not with the original purpose. So that's what we're trying to figure out here, whether the requestor can just go ahead and process the personal information based on further purposes that are not incompatible with the purpose that controller one originally collected the personal information.

But the thing is that those purposes are different. We have to keep in mind the work we did in phase one. The legitimate purposes for which third parties might seek disclosure are not the same purposes for which the controllers originally require collection of this data.

So, the question of compatibility and incompatibility with those original purposes, to me is not something that the requestor or the secondary controller should be determining on their own. It should be something that the primary controller should be determining.

So, that's really the issue to me, because the primary controller is the one who is accountable to the data subject. The primary controller is the one who will provide the data subject with access to how its data was processed. It won’t be able to do that unless it has access itself to a full audit of how this was done and this is not something that can be done if the secondary controller, the party to which the data was disclosed, does not inform or seek permission or guidance from the primary controller on how to further process this data.

Also, like I said, I think 5.1b does not allow for this to take place. I think that the requestor has to seek permission from the primary controller on any sort of further processing, and the determination of whether it is or is not compatible with the original purpose for which the data was collected from the data subject is a determination that also needs to be made by that primary controller. Thank you.

JANIS KARKLINS: Thank you. I feel that we are spending too much time on this without progressing. I have a feeling that we need … Maybe let Amr or Margie and who else wants to pop in to come up with a proposal that would address all those issues. Let me take those who have not spoken yet. Stephanie?

STEPHANIE PERRIN: Thanks very much. I wanted to echo what Thomas had written in the chat, that the recipient to the data is now the controller. The important distinction is that recipient has no nexus with the registrant who we ought to be considering the rights of as our first step, all the way through.

And absent independent oversight of what they're doing, what we have then is a new controller with a large collection of data doing things that they may consider to be consistent with the original purpose for which they requested the data from the other party, presumably the other party being ICANN. And I think while Brian might be speaking as a good lawyer would in advising his client, ICANN, to avoid liability, we have some very memorable recent data breaches where, for instance, Equifax sold client data, for which there is no nexus either with Equifax, to criminal gangs. This is the kind of behavior that we have to find a way to guard against, because it is the responsibility of the primary controller who has the nexus with the individual to ensure that there is a necessity test before they release data and that the recipient is responsible. You can't get around that. And this discussion of audit has to be some kind of independent audit. You cannot just say throw the … That that issue is now between the registrant and the secondary data controller. That is irresponsible. Thanks.

JANIS KARKLINS: Thank you, Stephanie. Look, I think we're overly theoretical here. Here in this concrete sentence, we are trying to address issue that business community raised, namely. When requestor states not only one potential reason why the data is requested but let's say two or three, this is not – requestor is not in possession of data. It is simply, the question is whether requestor can say, "I request this data for two reasons. Reason A and Reason B." The answer is yes or no. If answer is no, that means that requestor needs to file two requests, one for one purpose and another for another purpose.

So, how the data owner or controller will react, this is in the next building block that we will be discussing afterwards. Mark, your hand is still up. Please, go ahead.

MARK SVANCAREK: Thanks. You've covered the main point I wanted to make is that since we're talking theoretical things, it's hard to really nail this down. I made my point in the chat. Thanks.

JANIS KARKLINS: Thank you. Amr, may I ask you to keep working in light of this conversation and come up with a proposal which would meet also concerns of business community, Amr?

AMR ELSALDR: I'll certainly continue to work with Margie on what we would want to report to the rest of the team, but I think we've argued this to death a bit. I'm not sure that we can come up with a complete proposal to replace section C.

I wanted to make one clarification, though, based on your last comment, Janis, if I may.

JANIS KARKLINS: Yes.

AMR ELSADR: The one area that Margie and I do agree on is that if there are multiple purposes at the time of disclosure requests, that those can be submitted together. You don't need to submit two separate requests for data disclosure because you have two separate purposes. You should be able to include those in the same purpose.

Furthermore, I think one of the sentiments I expressed to her was that if the controller at that point decides that one of these purposes is legitimate and has a legal basis, then they would provide disclosure on that basis. But they find that the other purpose is the opposite, it is not a purpose that has a legal basis, that disclosure would still proceed and processing of the information would be allowed for the one purpose that is permitted. So that wouldn't get in the way of it.

I think that the real problem we're trying to solve here, which to me seems a bit … I think we're making a really big deal out of this when it shouldn't be that much of a big deal. The real thing we're trying to solve here is after disclosure has taken place, if the requestor who is now in possession of this data comes up with a new purpose that they did not disclose at the time of the original request to the controller, can the requestor at that point make a determination to process the data because they find that the purpose that they've identified after the fact is not incompatible with the original purpose for which the controller collected the data? This is where the problem is.

So, we've got one side of the argument saying yes they can and they should just go ahead and do it and the other side saying no they can't, they should contact the controller that provided the data first and take permission for that further processing. So that's really what we're trying to solve here.

So, either way, the requestor can get an answer to their question. It's just that this agreement is whether they answered this question themselves or they seek the permission from the controller that provided the data. Thank you.

JANIS KARKLINS: Okay. I think, from what you described and if everyone is in agreement with that, I think we can formulate maybe in a few, not in two points but in three or four points, splitting each of those issues separately. Let me then suggest that we will try to come up with a new C by Thursday and see whether, based on this conversation, and specifically what you just said, describing those issues, we would try to propose a formulation for C by Thursday. Hadia, I would like to go further to D, but since you haven't spoken, please go ahead.

HADIA ELMINIAWI: Thank you, Janis. I'll be really quick. I just wanted to note the importance of considering that each requestor would have an ID but each request for a specific purpose would have also an ID. That means that one single requestor could have multiple IDs, unique identifiers I mean, and each requestor could have multiple unique identifiers for multiple requests and purposes.

What I mean here, when you grant access or disclosure to an entity, you grant it to the entity for a specific task, for a specific purpose, and that should have a unique – it should be uniquely identified.

So, even if you have multiple purposes, and one single requestor, you wouldn't need to identify each individual request from a requestor with a specific – for a specific purpose.

I'm not sure that I was able to explain what I mean, but we should keep in mind that it is the disclosure is for a specific task for a specific purpose and that should be uniquely identified. Thank you.

JANIS KARKLINS: Okay, thank you, Hadia. So, let me move to subpoint D. Subpoint D, the requestor must handle the data subject personal data in compliance with applicable law, including keeping the record of processing activities where required. Any issue with this added statement? I see Marc Anderson.

MARC ANDERSON: Thanks, Janis. I don't have an issue with this and I think this is probably just a conversation that we should continue in the auditing section. But I think including keeping a record of processing activities where required is a little ambiguous, so I don't think we should get into it here. I think when we talk about audit requirements, we should be explicit on what record is expected, what processing activities, and get into how long that record needs to be maintained for, who and when those records could be disclosed to. I just wanted to point that out. I like that we've broken it out, auditing, into its own section and so I think we should get into the details there. But I just wanted to note that here.

JANIS KARKLINS: Okay, thank you. If I may ask staff to note those elements that Marc just said, to add in auditing section specifically on these things. Amr, please.

AMR ELSADR: Thanks, Janis. This is not an objection or anything. It's just a thought, really. I'm not clear on what the purpose would be for the requestor submitting a lawful basis for the processing to take place. The lawful basis here is one for the controller, so the controller has to have a lawful basis to disclose the personal information to the requestor. To me, it's the controller – or the discloser in this case – has to come up with its own lawful basis. So it's not up to the requestor to do this.

Now, the requestor can certainly provide their perspective on what that lawful basis for the controller may be, but I'm not sure what are we trying to achieve by requiring this during a data disclosure request. I'm just curious what others think about this. Thank you.

JANIS KARKLINS: Are you talking about subpoint B? Amr?

AMR ELSADR: Oh, yes, I think I was, actually. Apologies for that.

JANIS KARKLINS: Yeah. We are on D.

AMR ELSADR: Oh, my apologies. Yeah. I was referring to subpoint B.

JANIS KARKLINS: Yeah. I think we covered that. My recollection is that the requestor would state the purpose now, also possibly purposes, why he requested the data. But also, in his opinion, under which lawful basis this request should be dealt. That does not mean processor of the request will agree, necessarily, with the suggestion of the requestor. But I think we felt both could be stated by requestor for the sake of convenience of the processor of this request. Thomas Rickert helped me, saying that law enforcement agent/requestor must mention the legal basis.

So, on D, I understand that we can agree with this, with elements that Marc Anderson mentioned that would be captured in auditing section and we can color it green which would remain and we would need to work on subsection C or subpoint C and I see that Amr is volunteering to help us out and organize an online discussion on this until we get to the stable ground. Marika, please.

MARIKA KONINGS: Thanks, Janis. I just wanted to ask for clarification on D. So, is the agreement that we remove the language that was added, so including keeping a record of processing activities where required, and instead just put in bracketed language “see auditing building block for further details”. Is that what is being proposed, just so we get it right.

JANIS KARKLINS: My understanding is that we understand that this requestor will keep records on processing activities and that may be subject of audit, as for any other. Or maybe we can simply say that all these activities will be subject of audit as outlined in building block, whatever the number is. Would that be okay, if we would remove reference to auditing from each subpoint but would add like subpoint E, that all the activities would be subject of auditing as described in auditing building block.

So, let us move on now to the building block, next one, building block H, and see whether we can get [over] this one. So, on building block H, this refers to entity disclosing data. I would say that subpoint D, must log request, should stay in, but then we would have this logging. We need to make a reference to the logging building block. And the remaining issue is now subpoint H.

Subpoint H. So, any system designed for disclosing of non-public registration data to law enforcement authority must include a mechanism for implementing the need for the confidentiality of disclosure requests associated with ongoing investigation. For example, a law enforcement agency may exercise its right to [inaudible] entity disclosing the data to keep the disclosure request confidential while the investigation is ongoing and the system must allow for this.

So, this language was proposed, if I'm not mistaken, by Chris or in consultations with Chris. So, the question is whether we are in agreement with that. Chris, are you in agreement?

CHRIS LEWIS-EVANS: Sorry, me and James have been working on this after the separate small group meeting that we had a week or so ago. Unfortunately, because of other work commitments, we've not been able to complete this but we are pretty much there and I would probably hope to have it done certainly before the meeting. Thank you.

JANIS KARKLINS: So, it means that you are not yourself in agreement with this proposal. Not yet.

CHRIS LEWIS-EVANS: I don't believe that there is enough agreement across all the stakeholders to carry this forward.

JANIS KARKLINS: Okay. Let me take a temperature. James, please.

JAMES BLADEL: Yes. Just to echo Chris's statements and to note that part of that delay is on my side. Chris had sent some draft language, got caught in my spam filter, so apologies for the delay on this. Should have something for review by Thursday. Thanks.

JANIS KARKLINS: Okay, thank you. So, then I will not entertain discussion on this if the main proponents are not in agreement themselves, so then we need simply to wait. Let me see on … We maintain H in brackets. Let me see if we can agree on I, where not prohibited by federal law the disclosing entity must not disclose non-public data of data subjects that are clearly identifiable as a data subject protected under applicable data protection regimes. So, Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I think I get what this is trying to say but the use of double negatives here makes it a tad bit confusing. I don't know if there's maybe a better way to say this but I guess I'm okay with the spirit of what this is trying to accomplish.

JANIS KARKLINS: Okay, thank you. I think that the proposal came from the team member during the last call and this is captured by the staff. So, from a linguistic perspective, is there anyone who can – from native English speakers, who can help get rid of double negatives? Alan Greenberg, please.

ALAN GREENBERG: Yeah. Thank you. I can't because I don't really understand it unlike some of the people who said they get the gist but it's badly worded. Can someone put this in spoken description, not a formal sentence, to describe what it's trying to do? Because I really can't parse it enough to understand that. Thank you.

JANIS KARKLINS: Okay, let me try. If I understand it correctly, my understanding is that if there is a reasonable belief or reason to believe that disclosure of the data may endanger the data subject, and if that is not prohibited by the applicable law, then this data should not be disclosed. That relates to human rights defenders or dissidents or something like that. So this is how I read this text.

ALAN GREENBERG: Can we not say something like "data must not be disclosed if" and then give the reason? If it may harm the data subject, unless applicable law requires that it be disclosed. Something in a positive way, instead of negatives. I'm not sure that captures it properly, though. Thank you.

JANIS KARKLINS: Okay, Alan. Thanks for input. Mark SV.

MARK SVANCAREK: Yes. I'd like to do something akin to what Alan G is suggesting. I'm not actually sure that this wording says what you said, Janis. So I think we have to … I applied some Boolean logic to it, so I don't think it actually says what we intended to say. I think we need to rewrite it along the lines that Alan is suggesting. Thanks.

JANIS KARKLINS: Okay, thank you. Brian King?

BRIAN KING: Thanks, Janis. I'm not sure that this is our place to even opine here. If the law says that data in some cases can't be disclosed, the law doesn't require an ICANN policy to be a law. So I guess we could add something along the lines of a footnote, but I don't know if this invites more problems than issues, so I can table my concern until we see a rewrite of this, but this to me seems like an odd thing for us to be including in policy language. I would ask that, at some point, we go back up because we didn't start at the beginning of this use case and we have a comment on at least A, within building block H, if we could get to that at some point. Thanks.

JANIS KARKLINS: Yeah. Look, we have … This is already third or fourth reading of this building block and I thought that we have agreed on first, which are in red. But if I'm wrong, then of course we will go back to A. But let me take a few further inputs and then we'll go back to A. Chris, please.

CHRIS LEWIS-EVANS: Yeah. Thanks, Janis. I'm also a little bit confused. Look up what it was saying, compared to the new text, I'm agreeing that might have raised this before about unless prohibited must disclose the non-public data for data subjects, legal persons. I thought the text for this was to cross off the case I think it was Stephanie said about where that legal person's data has a natural person's name in it and I thought that was what we were trying to cover off here, but the language sort of straight into the whole "by protected person's" which is, as Mark has just said, has its own special protections around in lots of data protection laws. So, I'm a little bit confused about where this section is supposed to be going and the best way forward. Thanks.

JANIS KARKLINS: Okay, thank you. Stephanie and Thomas. Stephanie, please.

STEPHANIE PERRIN: Thank you. I think, actually, I take that point that Chris was just speaking about. I think we've gone off in two directions here. There is one thing about releasing a name and there is another about releasing the identity of a person who might be harmed.

Now, the Expert Working Group did quite a bit of work about this particular problem. It's one that the NCSG is fairly passionate about because we try to protect human rights defenders and political dissidents and women who argued for the right to drive cars in countries where it's forbidden.

It is very difficult for a registrar, I would suggest in responding to such requests from authorities that are in fact backed by law in going after such people to stick to the constitutional protections that appear in other jurisdictions and that's a fundamental problem that we have to grapple with. Are we going to fall to the level of local law or are we going to stick to GDPR-type protections that appear in the charter fundamental rights, not necessarily the

GDPR, but they are spelled out there and that is what the GDPR rests on.

So, I recommend that we split these two things. How we handle that other one, the protection of human rights defenders, is a very difficult problem and I think it requires possibly more reflection than we've done at the moment for the particular problem. Thank you.

JANIS KARKLINS: Thank you. Thomas, please.

THOMAS RICKERT: Thanks, Janis. Building on Stephanie's point, I think it's virtually impossible to base the system on local laws because local laws, in many cases, justify sanctions that are, at least in the view of most this group I guess is proportionate to [inaudible] that potentially has taken place.

So, I think that maybe a starting point for this could be … And I'm looking at our friends from the law enforcement and government community here, is that disclosure requests must not go further than where MLAT are in place because there are certain cases in which MLAT would not lead to the disclosure of data because the rights of the targeted individual are not secured with the legal system.

And if we then add in maybe a sentence about proportionality, I think we could make it work as policy language. The implementation, though, will be much harder, because I think in the absence of a clear legal internationally sound basis, it all has to take place within the balancing of rights, where you have to weigh the risk for the individual whose data is being disclosed against the rights of those who are requesting the data. Thank you.

JANIS KARKLINS: Thank you. Is there any volunteer who would like to try to reword subpoint I? So, no volunteers? Staff will do that. Thank you.

Let me now go to A, and I saw Brian suggested that … Can we have A on the screen? Brian suggested that in small a, we should strike “necessary”, that must only disclose the data requested by requestor. Any issue with that? Brian? Stephanie, I think your hand is an old hand. Brian, please.

BRIAN KING: Sure. Thanks, Janis. For the points I put in the chat, including that the word “necessary” in GDPR context does not mean strictly necessary and it has the risk here that this is interpreted differently or badly in the future. What this bullet is trying to do is just saying you don’t get more data than you’ve requested, and I think we all agree to that and we all agree to this bullet. The necessary data invites analysis and scrutiny and the risk of misinterpretation down the road, and if that’s gone, I think that’s a better bullet point. Necessary means necessary. That’s a legal thing, again. The law doesn’t require the policy to use that word in order for the law to apply, so I would strike it and leave a bullet there that I think everybody agrees on. Thanks.

JANIS KARKLINS: Thank you. So, is there anyone who objects deleting “necessary” in subpoint A? No objection, so that’s deleted.

So, on this building block, we have two outstanding issues here. One is an H where Chris will work with friends to finetune the point H and staff will try to come up with a proposal based on conversation we had on subpoint I. And as soon as we are ready, I will bring this for confirmation to the whole team.

So, with this understanding and in absence of request for the floor, let me now move to next agenda item, which is query policy, building blocks I and O. And if I may ask staff to put that on the screen. We unfortunately will not be able to devote more than 25 minutes to this conversation, so therefore please be as concise as possible.

So, EPDP team recommends that the entity disclosing data may take measures to limit number of requests submitted by the same requestor if it is clear that the requestor are not legitimate and/or from abusive nature. And with abusive, there is an asterisk. Then, explanation what that abusive nature looks like. And this is for sure not exhaustive list but gives an idea of what that is. [inaudible] submissions of [inaudible] or incompetent requests. Not use of [inaudible] formats during [inaudible] period is not [considered] system abuse. Frequent duplicative requests that were previously fulfilled are denied. Use of distributed or [inaudible] sources addressing platforms [inaudible] or rate limits. Use of fault or counterfeit credentials to access system storing, [relaying] and sending high-volume requests with the intention of causing [inaudible] or other parties to fail. [inaudible] of performance and attempts or efforts to mine or harvest data protected by [inaudible].

So, this is the non-exhaustive list that was proposed. I see a few hands up, starting with Caitlin. Then, Alan and Mark SV. Caitlin, please go ahead.

CAITLIN TUBERGEN: Hi, Janis. I just wanted to let the team know that – you will likely see the note in the margin but the text here was provided by James and that was in an action item to provide a non-exhaustive list of what abusive use could look like. And then in the bracketed text, support staff try to come up with some caveats that were added by Mark SV in response to James' list. So, the bracketed text was not included in the list. It was an attempt to reconcile some of the issues but Mark SV has not seen that, so I just wanted to clarify what that text was. Thank you.

JANIS KARKLINS: Thank you, Caitlin, for clarification. Let me take reactions. Alan Greenberg, please.

ALAN GREENBERG: Thank you very much. I understand the intent here but the descriptions here are, in many of these cases, are so highly subjective that I don't understand what our next steps are to end up with some uniform policy. What someone may describe as high volume certainly will vary based on the technical infrastructure that is being used to address them or the staff. I worry about, specifically about what we've described as bad actors using these to essentially cut off access or come close to cutting off access and I don't know how we implement them and get something which is less subjective. Thank you.

JANIS KARKLINS: Thank you, Alan, for your reflection. Mark SV?

MARK SVANCAREK: I agree these are subjective. I guess James and I were considering that we would get to more detail in the implementation phase, but if there is not comfort with that, then I guess we need to dig into this more specifically now.

My main comment is that I've never been comfortable with number six because those are undefined terms, so I'm especially concerned about subjectivity related to those undefined terms, mine and harvest. Based on my understanding of what's intended by mined and harvest, we already have coverage against those behaviors. You have to say what you're going to use it for. You have to only use it for what you say. You have to only keep it for as long as retention is allowed. I'm not sure what specific, detectable behavior we're trying to prohibit using these undefined terms, mine or harvest, so I think we need to discuss that bullet number six more completely before I could accept it. Thanks.

JANIS KARKLINS: Okay, thank you. Caitlin, your hand is still up, as well as Alan's. I suspect that you haven't taken them down. Greg, please.

GREG AARON: Thank you. I understand what the intent is of these but a few of them present some challenges. Number three, for example, talks about quotas but quotas is not a topic that we've talked about and its inclusion is problematic. And rate limits as well.

I'd point people back to SSAC 101 which says that if somebody is submitting a legitimate request, they have legitimate purpose, they have submitted a complete, properly formed request, that needs to be accepted and considered. But rate limiting and having one party decide how many another party can ask for is a problem.

So, I would suggest that three probably be deleted. The use of distributers [inaudible] source addresses is something that happens in current WHOIS but this system is going to be different and usage is going to be limited to certain parties – should be – and is going to be monitored very differently.

As someone else said, number six also contains some undefined terms. I think what we're after is maybe some sort of an understanding that we never had with WHOIS which was we tend to have the receivers of the queries, the contracted parties right now, deciding what frequency or number of requests they want to receive and having a unilateral ability to set limits. But that may not work in this system. So, three and six might need more work or deletion. Thanks.

JANIS KARKLINS: Thank you, Greg. James?

JAMES BLADEL: Hi, thanks, Janis. Just to respond to some of the comments that have been mentioned here today. This list – and I would point out that some of these terms that folks are not comfortable with are currently present in the 2013 RAA, so these are not completely alien in our space.

Look, I think there's really two ways to go here. One is to try to be as specific as possible and define exactly what behavior is or is not abusive. And the other one is to just kind of roll all of these up and say something along the lines of commercially – what's the term we like to use? Practical and commercially reasonable efforts to prevent abuse.

But I think that folks need to appreciate that while everyone on this call has always been a good-faith consumer of these types of data services, once they go live, including potentially SSAD, they are a big target and they have to have mechanisms in place, and perhaps not entirely public or transparent mechanisms to prevent abuse. As soon as we specify all of that in advance, we are handing a blueprint to the folks who want to break the system, knock it offline, or to otherwise perhaps misuse the tool.

So, I'm fine if we want to get super specific, I think that just invites folks to innovate around that and find loopholes. I'm also fine if we roll this up and just use those terms, like commercially reasonable. But what I'm not okay with is that we handcuff providers to an untenable, burdensome, or non-cost-effective obligation that a small registrar, for example, would have to respond to tens of thousands of requests every hour and they'd have to hire an army of folks just to serve their SSAD masters. This is also not something that we need to consider.

So, all of these things have to be proportional but I think some of the comments I've heard today have a very narrow perspective on how the system would be used by legitimate actors and perhaps a lack of imagination on how they can be misused by bad actors. Thanks.

JANIS KARKLINS: So, thank you, James. Next is Thomas.

THOMAS RICKERT: Yeah. Thanks very much, Janis. I think probably a way out of this can be to meet one of GDPR's requirements, which is that you need to have adequate technical and organizational measures in place, so-called called terms. In the legal world, you would typically not publicize those, in order not to disclose to potential attackers what measures you have taken to protect data.

So, I think one aspect would be to just require adequate terms to be in place. And the other thing I think we really need to have is some sort of volume control, because even requests that appear to be legitimate might be abusive.

I think maybe we can take a look at how registries are dealing with this. Even the pre-GDPR world, a lot of registries had voting limitations in place, either by number or where they had response times that would gradually increase. I'm looking at the tech folks on this call to maybe help with that.

But I think that having, in summary, a combination of technical and organizational measures plus some sort of volume limitation might do the trick.

JANIS KARKLINS: Thank you, Thomas. Honestly, I see that there is no disagreement in principle there. Some concerns. If we look at what is suggested here in point A is that if there is an obvious abuse of the system, then measures to limit numbers of requests that are submitted by the same requestor should be taken.

The second is, point B says, that we need to monitor a system and take appropriate actions in case of abuse of the system. The question is what constitutes abuse of the system. James volunteered to put non-exhaustive list. My question to the team is whether we need really to discuss any longer A and B as imperfect as they may be formulated but rather concentrate discussion on that list presented by James simply to progress forward.

So, I have Alan Greenberg and Mark SV in that order, please.

ALAN GREENBERG: Thank you very much. I think one of the key things here is that we need some reference to proportionate. We have registrars and registries, but registrars will be the main focus, that range in size radically. And a number of requests that is outrageous, for one, might be almost nothing.

I'll give you an example. We, earlier a few weeks ago, talked about one request per minute, which is roughly 1400 requests per day. The comment was made that seems sufficient. But if you look at a large registrar – and I'll use GoDaddy because the numbers are readily available – and just look at dot-com, if they were subject to 1400 requests a day, it would take 91 years to harvest all of their data. Clearly, not a practical thing.

So, a number that might make sense for a small registrar as being excessive is not for a large registrar and I think we need to build something like that into this, because a single number is never going to work, based on the huge radically large numbers of magnitude different in size between the various parties. Thank you.

JANIS KARKLINS: Okay. Thank you. Mark SV?

MARK SVANCAREK: I had two comments. One, there was a previous intervention about let's look to what we did in the past. I think Greg has raised some points that what we did in the past is not necessarily applicable, number three being a great example of that. If we're using credentials, then it doesn't really matter which source addresses we have, necessarily.

It's okay to look to the past, but I don't think that we should look to it too hard because it's probably not going to be applicable in many cases.

The other point, James made a good point that we should have great imagination in conceiving what bad requestors are going to do. We should also have great imagination to think about what bad registrars are going to do, and as he said, everyone here is a good faith actor, but we know that there are others who are not and so the idea that a very small registrar with a very high percentage of abused names would get some sort of a ripcord. "This is not proportional to me. I can't afford this." Even though it's possibly a problem of their own making. That's the sort of thing that needs to be considered as well.

So, just saying it's a tough problem. I'm not sure how we're going to implement it. This was our first attempt. Thanks.

JANIS KARKLIN: Okay, thank you. You see, I was born in Soviet Union and that was a repressive regime. It was interesting to follow a legislative process. And every law which was written in Soviet Union was written with the understanding that people would cheat. This is why society never had the sensation that this is your own country. Now I'm living in a country where legislators are writing the laws how they should be implemented with good faith and it was much easier to breath in the country I'm living now.

I'm saying this. I think we should write a policy based on common sense and how it should work, not with the knowledge that somebody will try to cheat. We need to have safeguards in and we need to punish those who will cheat. But if the underlying premise of the policy will be we know that it will be cheated anyway, so we will not get anywhere. With that, Greg?

GREG AARON: Just briefly. I think what a goal here is, is for both the users of the data and the suppliers of the data have a kind of a common understanding. In previous issues that have involved ICANN contracts, that was not always the case and I think that's what we're after. If both sides have an understanding of the expectations, it's also easy to figure out when you do have a problem whether it's abusive or not.

But proportionality in this case is going to be about both sides having a say in what might be abusive and understanding that both sides have some legitimate concerns. Thanks.

JANIS KARKLINS: Thank you. James and Volker.

JAMES BLADEL: Sorry, mute button was missing. Just to note that, to Mark SV, no need to be imaginative. We've seen bad registrars abuse these types of practices. For example, when someone wanted to transfer a domain name from their registrar to GoDaddy, we would see them say that we were abusing their WHOIS service, when we were in fact just trying to facilitate a portfolio transfer. So, I get it. There are bad actors on all sides.

The more I hear the concerns, the more I think that perhaps enumerating a list might not be the right approach and maybe we do just roll up and say that data providers will take commercially reasonable steps to prevent abuse of the SSAD system and leave it at that. Honestly, I think that starts to look a little bit more reflective of what we see in some of the original documents and some of the language that protected the previous WHOIS system. And maybe that's just the way to give enough flexibility and discretion to the providers, so that they feel like they can cover their bases. Thanks.

JANIS KARKLINS: Thank you. Volker?

VOLKER GREIMANN: Yes. Thank you, Janis. Just with regard to what Alan said, that it might take 91 years to harvest the entire GoDaddy database, I think it should take 91 years to harvest that because I can't imagine any legal legitimate purpose that would entitle someone to harvest that data by the entire database and have a legitimate interest there.

I think we need to make sure that there is not abuse, because in this circumstance, people have harvested the entire databases of WHOIS to use for spam and have been selling databases on the Internet and eBay to make sure that others [inaudible] spam with them as well.

There are certain patterns of abuse that have been recognized in the past and we should at least try to eliminate those, even though we might have other measures that also eliminate abuse that we haven't seen yet. But looking at what we've seen in the WHOIS, I think there are certain lessons to be learned that certain types of abuse have to be curtailed from the start, have to be disallowed to make sure that the system is not abused again.

JANIS KARKLINS: Thank you. I will entertain two further requests and then I will draw this conversation to conclusion. Alan Greenberg and Greg.

ALAN GREENBERG: Thank you very much. I'll be very quick. We are looking for allowing legitimate use, so that's clear. The challenge is, as James put out there, are going to be bad actors and what we need is enough clarity here so compliance can take action against them. Vague words will not allow compliance to take any action and that's been demonstrated really clearly in the past. So, we need to find some middle ground which is clear enough so compliance can take action against bad actors and do not act as an unreasonable load on legitimate actors. Thank you.

JANIS KARKLINS: I still have this feeling that we're forcing open door because what is written in A and B is what action should be taken. The question is how to determine abusive nature. What James tried to put non-exhaustive lists, what could constitute abusive nature. So, now we're going in circles and basically repeating our conversation that we had already during the previous conversation. Greg?

GREG AARON: To be clear, some of the things that James suggested are personally okay with me because they are clearly out of scope. Now, what Alan says is true, though. We do need to learn from the past and if there isn't something for compliance to sink its teeth into, then the language is not useful at all.

James had also suggested a formulation saying let the registries and registrars decide what is commercially reasonable and that's I think a non-starter, because it's completely one-sided.

Again, a small registrar might have 10,000 domains that are a problem and somebody may need to query those, and if they're creating a security problem, it's not just querying 10,000, but also doing it within a period of time that allows response.

And if the registrar has accepted those registrations, that is now that registrar's problem and they do need to serve those queries if they are legitimate.

So, using a commercially reasonable basis has proved to be, in the past, a really vague thing. It's created some compliance problems and I think it's one-sided. Thank you.

JANIS KARKLINS: Okay, thanks. So, I think we need still further conversation but I would like to suggest that we focus more on formulation on this term, what constitutes abusive behavior, if I may suggest and see whether we can agree.

Today, in the conversation, there were some concerns expressed with point 3 and point 6, so I would suggest maybe to continue our conversation on Google Doc trying to finetune formulations of 3 and 6. But my feeling is that no one really contests the substance of points A and B. The only conversation that we have is about abusive nature, what that constitutes. So, there was a suggestion also to put that response should be proportionate and maybe staff could think where that notion of proportionate response could be added in point A or point B or maybe additional points. Just thinking. So, we will revisit this building block I during one of the next calls, latest in Montreal.

With this, I would like to go to the next agenda item, that we can get some sense of proposal, how to deal with the priority two items. So, if I may ask, put the proposal on the screen and Marika to introduce the thinking.

MARIKA KONINGS: Thanks, Janis. So, what you see on the screen is a document we shared together with the agenda, based on some conversations on the list. Leadership team asked staff to have another look at the priority two items and see what next steps could be taken in order to move some of this work forward, recognizing that of course everyone is already pretty busy as well on the priority one topics.

As you may recall, we had a number of small teams also looking at these topics a while back and they also made a number of suggestions or recommendations. We factored those in the recommendations we provided here. If you click on the link, you'll also be taken to the worksheet which also contains all the background information on these topics and the discussions that have been held to date.

So, on the first topic – and Janis, I don't know if you want me to go through them one by one or whether just in a high level introduce them all and—

JANIS KARKLIN: Yeah, no, please go through all. We have 13 minutes to go.

MARIKA KONINGS: Okay. So, the first topic related to display of information of affiliated versus accredited privacy-proxy providers, and as you may recall, this was a topic that was discussed in phase one and there were some questions around if or how this issue may already be addressed in the context of the implementation of the privacy and proxy accreditation policy that was adopted a while back.

So, what we suggested here – and I think some of you are aware that that implementation is currently on hold, but we think it may still be useful to find out if or how that topic is specifically considered in the context of that work. So staff will take an action item there to check with our colleagues supporting that effort to see if or how it is already addressed there, and based on that input, basically come back with possible proposed next steps, if it indeed it is not addressed in the context of that work and it is something that this group may need to consider. So that would be a first concrete action item that staff could help move forward.

Then in relation to legal versus natural persons, that's also a topic that was discussed on the list. Coming out of phase one, there was a recommendation for ICANN Org to undertake a study on that topic to help inform further deliberations on this topic. So I think first step here would be for us to confirm with our colleagues who are responsible for the implementation of that study what the status is and what timeline they have in mind in producing the results of the study, and again we hope to get a response on that pretty quickly.

There is, of course, as well some work that will need to be done on the scoping of the study and there are a number as well of legal questions that were identified, so we suggest as well that in parallel to this study being undertaken and clearly understanding what the study is expected to address and answer, for a legal committee to already start looking at what questions, if any, can be submitted or should be submitted prior to the completion of the study.

Then, of course, once the results of the study are in and if there are any further legal questions that needed answering to help inform those deliberations, that would then of course serve the basis for the EPDP team to consider whether or not any changes would need to be made to the recommendation that was made in phase one in relation to the treatment of legal and natural persons.

In relation to the city field, redaction, as you recall, that was also a topic discussed in phase one and there was legal advice that came in very much at the end of the process. There was agreement that should be further reviewed and analyzed to determine whether or not that recommendation needed modification. So, here, our suggestion is that the legal committee reviews and analyzes that legal advice and basically takes that [inaudible], recommends next steps to the EPDP team which could include, based on their review of the legal advice and modification to the phase one recommendation. It could recommend maintaining the recommendation as is or there may be additional legal questions that rise from the review that are needed to be answered before the legal committee can make that recommendation to the full team.

In relation to data retention, as you may recall, there was also an action item here for ICANN Org to document ICANN Org's processes and procedures, and on that basis indicate whether or not the data retention periods that were recommended in phase one were sufficient or whether potential changes will need to be considered by the group, so here an action item would be for staff to confirm what the status of that work is, and of course once that review is received, the EPDP team can consider what, if any, updates are needed to the phase one data retention recommendation. And of course that's dependent on the delivery of the ICANN Org review.

There was also an action item or recommendation in relation to the potential use of data by ICANN's OCTO team. Our suggestion would be here that we follow-up with our colleagues to determine whether the status of the input that was provided during phase one has changed or whether there has been any legal guidance obtained in relation to ICANN Org having a qualified resource position under GDPR. And I think as some of you recall, it was something we discussed in phase one as well. Then, based on the feedback received from that query, the team would consider what the appropriate next steps are in relation to that specific topic.

Then, there was also a topic in relation to the feasibility of unique contacts to have a uniform, anonymized e-mail address. This is one of the topics that appeared in the annex to the temporary specification. Our suggestion is here that the legal committee would review the questions that have been proposed in relation to this topic and what is the feasibility of having a uniform, anonymize e-mail address. Again, an action here to look the work that some have already done on these questions and for the legal committee to determine which of those should be submitted to legal council for the group to have an informed discussion on this, and once that legal guidance is received, the team could look at that and decide next steps.

Then, lastly, there was also a topic of accuracy and WHOIS accuracy reporting system. As you may be aware, this is also the subject of a discussion that's taking place between ICANN Org and the GNSO Council and [inaudible] include the different letters that have been exchanged on this topic here, trying to understand what the exact scope of work is in relation to this topic, what the exact status of the accuracy and WHOIS ARS system is. So our suggestion here is to weigh the outcome of the discussion that's taking place between ICANN Org and the GNSO Council as that will likely provide more specific guidance to the EPDP team on what the expectations are from the Council's perspective on what needs to be done in relation to that topic.

So, that's it in a nutshell what we're proposing as next steps on these items in an attempt to try and start moving these forward. In parallel to the work that's ongoing in relation to SSID, as you've seen, there are a couple of items for staff to get information that will hopefully inform the next steps for the EPDP team, but there's also quite a bit of work that may be assigned to the legal committee, which of course is also still working on SSID-related questions. I think that's something for the group as well as the legal committee to consider how they can work that into their timing and prioritize their work accordingly, of course also in light of budget availability and the input that the board has provided in making sure that money is wisely spent and making sure that if information is already available to inform these discussions that that information should be used and not necessarily repeat questions being asked.

So, I think that's at least what staff has put together. I know you probably haven't had a lot of time to look at this. Of course, if anyone has any initial input, but maybe we can put in a deadline by, I don't know, the end of this week for people to raise any objections with these proposed steps, and if [inaudible] are made, we can at least from a staff side start moving these forward and also start lining up these topics for the legal committee as appropriate.

JANIS KARKLINS: Thank you, Marika. Without hesitation, I can tell you from staff side you can start moving forward already without asking the team because all the questions that you raised for yourself are very, very pertinent. And as it is usual in life, it is easier to ask for pardon than permission. With that, I see Brian's hand is up. Brian, please.

BRIAN KING: Thank you, Janis. I admit that I haven't followed the IRT as closely as some others on the EPDP team have, so I might have missed this. Is the IRT taking on that study? Is the IRT working on the study with ICANN Org or how is that being addressed now? Would be good for clarification. Thanks.

JANIS KARKLINS: Thank you. Marika, can you clarify?

MARIKA KONINGS: Yeah, thanks, Janis. My understanding is – and I hope my ICANN Org colleagues will correct me if I'm wrong on this. As the study is not dependency on the implementation of the phase one recommendations, priority has been given to getting that done as there are of course specific timelines that were associated with the implementation of the new policy.

So, I know that staff colleagues have already done work on this in the background, but it hasn't been brought to the IRT or the EPDP team yet, recognizing that work is going ahead full speed on getting the recommendations implemented on the phase one side, as well as the priority one items on this side. But I think our colleagues stand ready to engage with both groups but I think they're hoping as well to get some direction, get some indication, when everyone is ready and not holding up other work that has been flagged as priority number one.

JANIS KARKLINS: Thank you, Marika. I think if the team would be in agreement, to have a lunchtime conversation about terms of reference of that study, we could try to organize that on Saturday during our meeting in Montreal when [inaudible] invite ICANN Org respective staff to come in and brief us on thinking they have on terms of reference. Maybe while chewing food, we could also provide some immediate reaction, if we could think of half-an-hour, 45-minute engagement during the lunchtime with food in front of us, maybe that would be useful or worth to consider.

So, any other reaction or question to Marika in relation to proposal? I see none. Then, please, by end of the week, if you have any objections or any violent disagreement with proposal, please make it known on mailing list or on Google Doc. And if no objections will be received, staff will proceed with action items they have identified for themselves and we will then revisit issue in [inaudible] of information obtained.

So, with this, and taking into account that this is two minutes before 6:00, I would like to thank all of you for active participation in the meeting. Again, we have made some progress but not as much as I would like to, and nevertheless I encourage everyone to keep trying and look at the documents probably prior to the meeting and if you have any kind of systemic disagreement, please let us know prior to the meeting, not during the meeting.

That would allow us maybe to focus discussion differently or arrange discussion differently than we do.

So, with this, I will forward questions to ICANN Org on my behalf and we'll seek input by Montreal meeting. Other action items, Caitlin, as usual we'll circulate after the call as well as agenda. Alex Deacon promised to provide input as soon as possible on accreditation and maybe we will wait that input prior publicizing the updated version of accreditation, not to confuse team members and see whether there are any changes that need to be done as a result of [inaudible] of their proposal.

So, with this, thank you very much and I adjourn this meeting. Have a good rest of the day. Thank you. This meeting is adjourned.

TERRI AGNEW: Thank you, everyone, for joining. Once again, please remember to disconnect all remaining lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]