MONTREAL – GNSO - EPDP Phase 2 Meeting (1 of 4)
Saturday, November 2, 2019 – 08:30 to 18:30 EDT
ICANN66 | Montréal, Canada

UNIDENTIFIED MALE: It is Saturday, November 2nd, at 8:30 in the morning. This is the GNSO EPDP Phase 3 Meeting 104 at ICANN66 in Montreal.

JANIS KARKLINS: Good morning. Welcome to Montreal, to our face-to-face meetings. Seems that this is then 29th in a row that we have from the beginning of the process. Since we are on Zoom and we will be using Zoom also for establishing the line of speakers, maybe we would skip the presentations but then Terri will take the presence from the Zoom room.

We had a first initial conversation on the previous call about the agenda for the Montreal meeting. Now it is on the screen. We have in total four team meetings and then we have a plenary meeting with the community on Monday. Today we're working a full day with a few coffee breaks and a lunch break. During the lunch break, we will have a working session with ICANN org.

Then, on Sunday (tomorrow), we're meeting at 5:00. We will maybe briefly walk through the presentation for the community session and we'll continue plowing through outstanding issues of building blocks.

Then, on Monday, we have a session starting from 3:15, which is split in two parts. In the first part, until 4:45, we will continue working on building blocks and maybe policy recommendations. Then, for the second session, from 5:00 until 6:30, my suggestion would be to convene a Legal Committee meeting because the Legal Committee has not met now for a while. Those folks who are not on the Legal Committee maybe we could gather in another room to talk about a few outstanding issues that need some group work and further reflection in preparation for bringing them back on Thursday when the group will meet for the last time during this Montreal meeting. So we'll see whether that group work could be adopted by the team as a whole.

Thursday's meeting will be chaired by Rafik, since I will be leaving Montreal on Monday. I'm on vacation now, literally. For me to spend two days in lovely Montreal without doing nothing on my vacation? I would prefer to come back to Montreal during summer time rather than in November. So that explains why I will not be present, in person, Thursday. That said, I will follow the meeting online and will be present from Geneva.

So this would be the outlook for the week. Any comments? I hope that we have Zoom ready. I will try to copy it.

Today, if we can scroll down the screen, for this morning meeting, my suggestion would be to engage with the Strawberry Team since the document and questions of the Strawberry Team have been formulated and sent to the European Data Protection Board. The aim would be to

ask questions and clarify if something else could be done in that respect. Then we would go straight to the building blocks.

The order that I would suggest at [inaudible] was shared on the mailing list a while ago. We would start with the accreditation, hoping that the accreditation building block would be stabilized this morning.

In the meantime, I was alerted that some homework, some assignment, have not been accomplished in relation to the accreditation building block and others. So my encouragement would be to use maybe the coffee break, those who have not been able to accomplish their tasks, and try to finalize them because this is really crunch time if we want to meet our ambitious goal to submit initial reports by early December. Then we need also to really progress and then maybe change a little bit our working method in the sense that we address only outstanding issues, rather than doing a third, fourth, or fifth consecutive reading of the same document and revisit issues that we have already discussed and stabilized.

In that respect, I ask staff to color the text that we will see on the screen of building blocks. Every text or part of the building block that has been stabilized will be indicated in green. Only outstanding issues will be indicated in black and red. Red is the editorial suggestions that have been put in the Google Doc.

With this, can we accept that program of work for this week and the methodology, as I suggested?

Stephanie, please?

STEPHANIE PERRIN: Thanks. I just wanted to put a marker down, that our ambitious schedule is a bit too ambitious, and, if we attempt to achieve it by December, inevitably there will be a failure to reach consensus on some items because, once you put the building blocks together and make your selections, then all the other things change. At that point, you lose consensus. So I just think we're being a little optimistic and that Plan B ought to be somewhere, even if you don't put it on the table at the moment. Thanks.

JANIS KARKLINS: I think that humans by nature should be optimistic. Otherwise it would be very hard to live. Of course, life may bring some changes. I think, in certain respects, we have already indicated Plan B I think a month ago or less in one of the meetings (actually, it was the last meeting, the Los Angeles meeting): if we will not be able to meet the deadline of early December for submission of the initial report, which then would allow us at the end of the January face-to-face meeting to go through and review the comments for the initial report. In that case, we would aim at concluding our initial report or consideration of the initial report during the face-to-face meeting at the end of January, but also with the understanding that, in the meantime, we would take up also some Priority 2 issues and would try to add Priority 2 issues, either all (ideally) or a few of them, to the initial report. So that's Plan B. I think that that was something that no one contested as an option.

In absence requests – I'm now in the Zoom room; I have all the requests in front of me – I will now go to the first sub-item of our session, and that is the interaction with the Strawberry Team. I welcome Elena to our meeting and would invite you to take the floor to brief us on where we stand and what the team should know. Please.

ELENA PLEXIDA: Thank you, Janis. Good morning, everyone. Thank you for having us again with you. In line with what we had previously discussed and described to you, ICANN org drafted the paper, outlining a hypothetical model for access to non-public gTLD registration data.

The paper, titled "Exploring a Unified Access Model for gTLD Registration Data," was sent to the European Data Protection Board on October 25th, after several iterations with the European Commission, who provided invaluable advice on the paper overall and helped draft the questions, included in the paper.

The model outlined in the paper proposes that ICANN org takes on the responsibilities associated with a central gateway through which requests for access would be accepted and processed. The model outlined in the paper is a hypothesis. The paper notes that assumptions made therein are for discussion purposes and that the EPDP team will make its own policy recommendations. The paper also emphasizes that the structure of the model, if any, would depend on the EPDP team's recommendations.

But, that said, you need a hypothesis. You need to present a concrete-as-possible hypothetical model to the DPAs in order to get any meaningful feedback. This had been pointed out several times to us by both the European Commission and the data protection authorities themselves. You cannot ask in the abstract, "Do you think we could consolidate responsibility around the centralized model?" All you can get back would be, "Look at Article X and look at Article Z."

With this hypothetical model, ICANN org seeks to address and help clarify the legal foundations upon which any model for disclosure could be built. As you deliberate your policy choices going forward around SSAD, seeking this guidance, I note, is in line with the goal given to Goran by the Board to continue to work towards obtaining legal guidance from the DPAs as to whether a UAM is permissible and compliant with GDPR and also with several communications addressed to the Board and to the org, calling for a uniform access mechanism for registration data.

When we met in L.A. in September, we did say we were having a meeting with the European Commission in one week's time (the following week) and that we would update you after that meeting or you would hear directly from the European Commission when we hope to have a better draft. We did [inaudible] from the European Commission, we would start including the questions.

We are sorry you did not receive the paper before it was sent to the European Data Protection Board. Drafting was more challenging than anticipated. As I said, there were several iterations with the European

Commission, several bucketfuls. We were running behind the schedule, risking that the European Data Protection Board will not have the time to consider the paper even before the December plenary. For that reason, for timing issues, apart from us submitting the paper to the Board, I believe Georgios has already shared with you that the European Commission shared it with the Belgian DPA.

Now, turning to substance, we have described to you three questions we had in mind back in L.A. Over exchanges with the European Commission, in addition to those three questions that were properly formulated, two additional ones were added. These are Questions 1 and 5 for your reference. You might have noticed that the questions really revolve around the responsibility issue and the controllership relationship in combination with the joint and several liability provisions of the GDPR.

If I may put it in my own words, these questions, I believe, are very close to the questions that you're asking us. We are again, in my own words, in a chicken-and-egg situation that has been building up. We do hope that the answers that we will get from the DPAs will help set extra light.

Now that's with respect to the paper. Aside from the paper itself, with respect to engagement with DPAs, I would like to bring to your attention that ICANN Compliance has received a complaint from a European data protection authority against the registrar.

Now, what happened is that the DPA had received a complaint by a data subject concerning a GDPR breach about a website that was publishing the data subject's personal information unlawfully. The DPA needed to

contact the domain holder to inform of the breach and any follow-up actions to remedy this. Thus, in terms of the registrar, it provided the legal basis, with is Article 55 of GDPR. For reference, this is laying down the investigative powers of the DPAs and also establishes the legitimate interest. But the registrar denied providing the requested contact information.

So the DPA considered that this is not a provision of reasonable access as required by the temp spec since there was a clear legal basis and there was a clear, legitimate interest and turned to ICANN Compliance.

Now, I had a phone conversation with a handler of the case. She not only confirmed that this is obstructing an ongoing investigation and the possible for the remedy subject, but she also said to me that she has some 40+ similar cases sitting on her desk. ICANN Compliance is into it.

I just wanted to bring this to your attention. Thank you for listening. I'll turn back to you, Janis.

JANIS KARKLINS: Thank you, Elena, for this update. The floor is open for any comments or questions the team may want to raise with respect to the report.

Milton, please?

MILTON MUELLER: I read through the Strawberry Team statement. I appreciate the fact that they tried to emphasize very hard that the EPDP would be making

the policy, but I still have some questions about the assumptions that seem to be embedded in the questions.

For example, on Page 17/18 of the report, you say that a UAM would remove responsibility from the contracted parties for the specific acts of deciding whether or not to disclose the data. That's one of the issues that we're debating as a policy matter. It's probably the biggest issue. It's not something we've decided.

As you probably know, some of us see the centralized gateway as simply a way to make the request process easier and more sufficient for the requesters and not necessarily as something that removes responsibility from the contracted parties.

The other related question is on Page 20. There's a statement that, in ICANN org's view, a UAM is only viable if the assumption that a disclosure-related responsibility can be consolidated within a centralized system is correct.

Again, this is problematic in two ways. Number one, I don't necessarily think the UAM is viable. Again, there's an efficiency gain from just having a centralized system, even if the responsibility remains in the same place. Secondly, the whole document really never says where the responsibility is consolidated. I know that's not your issue. That's ICANN org's issue. But I'm not sure how the Data Protection Board is supposed to talk about that when it's so unclear on who they're talking about being responsible, ultimately.

I guess I'm asking this question more to the Strawberry Team, to the EPDP team: What kind of answers are we going to get to this, and does this presume away an issue that we really are actively still debating?

JANIS KARKLINS: Thank you, Milton. Any other comments? Reactions?

Georgios? We need to either use the Zoom room or the name plates. One or another. Raising hands is maybe not the best thing. So let's then try with the name plates. If that will not work, then we will move to the Zoom room.

Alex was first, and then Stephanie, then Georgios, and then Thomas.

ALEX DEACON: Thanks. Good morning, everyone. I think, in terms of Milton's question, we haven't made that decision. But I believe the reason we haven't made that decision is because we were hoping to get some guidance from the DPAs or the European Data Protection Board to guide us in the right way on whether this is actually possible or not. So we've been putting off that decision until we receive some input from the experts. So we're stuck in this hamster wheel a little bit.

It seems to me that the response – hopefully it's a helpful response – from the authorities that we may receive in the future makes it easier for us to finally answer what I think is a quite foundational issue for us and helps us make fast progress after that. Until we get some indication from the DPAs, it's not clear to me that we'll be able to truly make

progress. It's important that we be able to answer these questions. We're not there yet.

So I'm hoping – again, I'm an optimist – that their response, when it does come, will give us clarity on what direction we need to go and what assumptions we can or can't make. Thanks.

JANIS KARKLINS: Thank you, Alex. Stephanie, please?

STEPHANIE PERRIN: Thanks very much. Just for the record, I too an optimist or I wouldn't be here working still after six years. I really think we can do better.

I do think it would have been helpful to have put the draft document before us. If it was sent to the European Commission, I would like to ask – here's where my question is – which part of the commission? It's a big place. I'm presuming the telecom regulators who regularly are in battle with the DPAs over their regulatory efforts. So that's my question.

I think that I agree with everything my colleague, Milton, said about embedded thing. It's what I used to refer to as regulatory grooming, sending in a document that has all of your desired outcomes embedded, even with caveats. So I would have appreciated the opportunity to annotate that and indicate just how uncertain these outcomes are.

Anyway, there's my question. Who did you talk to at the commission and what was their input? We'd like to see that, too. Why are we working

here if we can't see what's going on? I'd like to know what the telecom regulators said because we know what they want.

JANIS KARKLINS: Thank you, Stephanie. Georgios, please?

GEORGIS TSELENTIS: I would like first to say, in all this procedure, I see a value when we were discussing in Los Angeles that we have this chicken-and-egg every time of the different parties that might be engaged in this centralized model, that they're hesitant to take some position about their responsibilities they want to take on this model without knowing exactly how this role will be interpreted by the data protection authorities. Already then I think we were, as the GAC but also as the European commission, saying it would be useful to formulate some questions and then try to get some answers. We know that this exercise is very complicated in the sense that you need to make some assumptions.

Now, at a certain point, even already in these questions, if you see, for example, the footnotes in Page 21 of the questions, there are different scenarios about how the model can treat, depending on the joint responsibility of the data process [and] also the data controllers. Again, I'm not on the side of the data protection authorities, but I believe it would be very useful even if they give some sort of reply for the different possible scenarios. It would help us disentangle the hold situation that is in front of us because we, as I said, have all the different players here that are hesitant to admit a clear role of responsibility.

Now, to the question, because it was a question also for us from, of which part of the European Commission. As far as I know, my colleagues from DG Justice, which are the ones who were behind the data protection legislation, we tried to use in this process as the intermediaries [as a model here and an informal opinion] because, as was explained before from Elena, before you have an official answer from the Board, you have already a discussion. It sense, it was the Belgian DPA who was approached [by] this model by the colleagues [at] DG Justice.

Again, I think it's useful even to have informal replies, even to have any type of reply. In this respect, I think we should also keep the expectations to a certain level. I don't expect, in all those questions we have put, straight answers because they are not straight questions in many cases. They have a lot of conditions attached to them.

Anyhow, I think it would be a very helpful exercise for us to get some sort of guidance that will move this exercise faster than having us debating around these questions and not reaching a consensus. Thanks.

JANIS KARKLINS: Thank you, Georgios. Thomas?

THOMAS RICKERT: Thanks very much. Hi, everybody. Thanks, Elena, for coming to us and visiting us. Sorry we have to ask some questions. I've stated already in

the call that I think it was most unfortunate that we didn't see the document before it was dispatched.

There are a couple of assumptions in the document. For example, on Page 17, it reads that ICANN is taking responsibility for the operation of the central gateway.

Is that the position that has been agreed on by the Board and by ICANN org? In other words, can we rely on this assumption that ICANN is actually willing to take responsibility for a central gateway or whatever we might call it in our scenario? Can we take that as basis for our work to build on? Because I guess that would be an answer to a question that we tried to get an answer for for months, if not years. It's surprising and refreshing that we get the answer through this channel. If you can't answer that, maybe our Board liaisons can answer that.

Also, in the footnote, there's the question for the European Data Protection Board to answer the question about joint and several liability. I think that's a nice way to not use the words "joint controller," but are we to assume that, if the European Data Protection Board confirms, as they, I think, did previously (that we have a joint controller situation), ICANN org and the Board will accept that so that we can take that as an assumption or as a basis for our deliberations?

The third question that I have is whether you had legal counsel advice in drafting the document to inform the drafting of this paper? If that were the case, then I think we would all like to see the advice that you got in order to inform our deliberations. Thanks so much.

JANIS KARKLINS: Thank you, Thomas. Please remember that the ICANN CEO also has invited us to think of if there is any questions that the team would like to ask the European data protection authorities and channel those questions through him to be submitted to the data protection authorities. I think that, if we have any of those questions, then they should be formulated as a result of today's meeting. Please think about them.

I have next Milton, then Hadia.

MILTON MUELLER: I just have to push back against this idea that we have this chicken-and-egg situation here that can only be resolved in this way. Here's how I see the situation. The European Commission and many other stakeholders have said, "We think a centralized system of access would be better." Now ICANN has presented us with a report that says, "If you want a centralized system, it has to consolidate liability or responsibility." They avoided the word "liability." But it doesn't say where it consolidates it.

Furthermore, that assumption is false. You can have a centralized system of access that leaves responsibility in the hands of the data controllers (i.e., the registrars). You can. This is fact. Nobody can tell me that you can't have that.

So we're presenting the Data Protection Board with a false assumption and saying, "Answer this question," which is still a little bit vague. So what kind of answer are we going to get? How's that going to help us?

And, as Thomas has pointed out, ICANN itself has not been terribly forthcoming on whether it is willing to take responsibility should the Data Protection Board say that they would have it. So that's holding us up than any kind of chicken-and-egg situation related to the understanding that is expressed in this paper.

So I really view this as a distraction at this point. I think we can, as a matter of policy, decide who's going to make the ultimate disclosure decision. We can make that decision. If the European Commission says, "If there's a centralized system, somehow the responsibility lies somewhere else," then that might be useful input after we've made that decision, but I don't see anything stopping us from confronting directly the question of where we want responsibility to reside for the disclosure. And we do not have to rely on these vague questions about whether the existence of a centralized mechanism for disclosing in any way affects that.

JANIS KARKLINS: Thank you, Milton. Hadia, followed by Mar[c].

HADIA ELMINIAWI: To Milton's point, actually I don't see this document making any kind of policy decisions for us. The fact of the matter is we are not able to make our policy decisions because of the legal uncertainties that we are

facing. So what I see this document doing is clarifying the legal uncertainties that are not allowing us to make our policy decisions. Actually, this clarification or maybe those kinds of questions should have been put out a long time ago, maybe before that. So thank you for letting out those questions because we do actually need the answers.

As for the liability and where does then responsibility for disclosure lie within the presented document, as I understand it, it lies within the centralized system. That would be among the three elements of the centralized system, which would be either the gateway, or the identity provider, the authorization provider, somewhere within the centralized system.

The part with regard to the registries' and registrars' responsibility with regard to the disclosure and not to the other elements, according to the presented document, if they actually transfer the whole data, they're not aware of the requester and they are not part of the decision-making. Maybe the responsibility for disclosure does not lie with them. But then we don't know. We still need to get the answer.

I think there was one more point, but I can't remember it. Anyway, that model allows for the data subjects to have a predictable system. I don't know why we are just ignoring this part of the system or that benefit of the proposal because it is obvious that it provides the data subjects also with predictability. They would know when and how their data could be actually disclosed as opposed to having it [lie] with the contracted parties. There could be differences among the registrars and there could be some kind of inconsistency. Thank you.

JANIS KARKLINS: Thank you, Hadia. Marc, followed by Farzaneh.

MARC ANDERSON: Thank you, Janis. I just had a follow-up question on timing. It sounded like, from your update, you were saying that, on the timing of it, you were hoping to get this in front of DPAs by their December session. Do I have that correct? So I'm wondering – obviously, at this point, any type of input or feedback we can get is useful; we welcome any kind of input – what kind of timing you're looking at and any expectations you have around that. Thank you.

JANIS KARKLINS: Thank you, Marc. Farzaneh, followed by Georgios.

FARZANEH BADII: Thank you. I just wanted to make the point that – I have made this point when we asked legal counsel questions as well – if the DPAs say something is possible, it does not mean that this group is going to agree on that point. So, just to make it clear later on, the basis of our argument cannot be said as, "Oh, but the DPAs say that this is possible, so we should do it." This is my fear, that, later on in the group, we will have people that just refer to these responses and say, "This is the basis of our policies," because it is possible we are going to do it.

I think the problem with the questions is that they are based on [that] some of the assumptions are false and some of them are policy assumptions. So that's just one point [inaudible].

JANIS KARKLINS: Thank you, Farzaneh. I think the group will make a decision based on its own consideration. So whatever answers will come will inform our discussion and not more than that. But certainly we want to avoid the situation where we develop a model that is unworkable and not compatible with the GDPR. So that is also something we do not want to do.

I have Georgios, followed by Stephanie and then James.

GEORGIOS TSELENTIS: Again, following what Thomas said regarding ICANN['s] meeting in the paper that they are taking these responsibilities of a central system, this is something that I said already in the face-to-face in Los Angeles. We are not taking about responsibility by a system or by somebody operating a system. If we want to talk to the DPAs, we have to talk in the same terms that they are doing their legal analysis with. The legal analysis is in terms of processing activities. We have to break down in this system what processing activities are we talking about, whether those processing activities involve personal data, and then who is the processor and who is responsible for this processing activity.

For example, in this system, it is described in the paper that we have authorization or identification or authentication, and all these are

distinct processing activities which can be described in the best detail we can agree upon at this stage. Then we should see who are the actors of those processing activities. Then, if, in this system, we say that the actor for this is ICANN or is another central entity, then we can go down and assign the responsibility and the liability accordingly.

So I think we should go [in the way] of an idea that we have a central system, we have an operator of a central system, and therefore automatically we assign responsibility and liability for this. We have to break down the details of this. The more clear we are about that, and the more clear about the actors and what sort of responsibilities they want to take in these processing activities – if it is the contracted parties, if it is ICANN, if it is another processor or controller – then we can have the answers probably more straightforward than answers from the DPAs. Thanks.

JANIS KARKLINS: Thank you. I have a long list. Stephanie, James, Becky, Margie, Alan, and Mar[c], in that order.

STEPHANIE PERRIN: Thank you very much. I just wanted to point out that this is a multi-stakeholder community and some of us, namely our constituency, might have different goals in consulting the DPAs. In other words, they might actually want them to support user registrant privacy right, not sort the liability issues for the contracted parties and ICANN. We recognize the importance of that issue. However, we're more

concerned with human rights; hence our desired to be included in any document that might actually go to the DPAs, which I still consider to be regulatory grooming if you're setting out something like that.

Now, my point actually is one that I was hoping the contracted parties would make, but since they didn't, I have raised my flag again. My understanding is that, if you're serious about investigations, you actually need the deeper data that is not going to appear, we hope, although we don't know this yet, of course, because we haven't got our data elements on a table yet. But we would hope that then IP address and the financial data and any other ancillary data that the registrars would have as the link with the registrant is useful in criminal investigations, which we seem to talk about a great deal.

Now, is there any way that ICANN is going to take on the liability for the disclosure of that data? Are the registrars and registries prepared to accept ICANN's due diligence before they release that next level? Or are we setting up two processes – one the progeny of the former WHOIS, shall we say (the SSAD) and then the deeper level of analysis? Thanks.

JANIS KARKLINS: Thank you, Stephanie. James followed by Becky.

JAMES: Good morning. Welcome, everybody. It's my first time in the queue so I just want to say hi. The conversation has moved on quite a bit since I put my flag up, so I'll just respond quickly to a couple of points.

Stephanie, you're correct. We've always maintained that the really good stuff has never been in WHOIS and was always available to law enforcement through due process, like warrants and things like that. I don't think that's what we're here to solve, not through SSAD or any of the systems that are under discussion.

To respond to Milton regarding whether or not any of this is really essential to our work, if we want to, from a policy statement, say where the decision and the responsibility lies, we can do so. Well, let's do so. I think we've all said, "We want ICANN to make this decision. We don't want ICANN to stand in front of the contracted parties and take responsibility for those decisions." I think, from our perspective, from a liability perspective, that's what we'd like to see. We certainly don't want a situation where we're responsible for decisions that are occurring elsewhere. I think that is understood, that we cannot accept any model that puts us on the hook for decisions made by some other system.

The problem is that I say is that the Strawberry's Team work is on the critical path for our work because it's a cliff at the end of it. If we go over the cliff, it doesn't matter how perfect our model is; we have to start all over. Maybe I can't speak for everyone, but I personally don't want to do this twice. So I would say, yes, it is important and I am grateful for this. I just would ask, from a process perspective, that we be included at the front end regardless of timeframe because we're working in parallel on so many of the same questions that we're sending to the Board, we're sending to org, and that org is sending to the DPAs. There's so much overlap here. I feel like we're chasing our tails.

JANIS KARKLINS: Thank you, James. Becky?

BECKY BURR: I just want to say there is a chicken-and-egg problem here. You've asked ICANN, you've asked the Board, some questions. We need some information to provide those answers. Assumptions had to be made, but clearly the policy development responsibility lies in this group. It lies in the community. That's where the bylaws put it. Nobody can take that away. So, unless, as James said, we wait until the very end – you develop a policy and then we go to the DPAs to ask if it works – we could be here for the rest of our natural lives.

So I understand that this is not perfect, but I don't see from a timing perspective how we could actually wait until this group finishes developing policy to then go the DPAs to ask whether it works. We had to get information.

JANIS KARKLINS: Thank you, Becky. Margie followed by Alan.

MARGIE MILAM: Hi. Good morning, everyone. As I think about this conversation, I recall where we started. At the beginning of this process, the contracted parties expressed their concern about liability, so we came up with the temp spec. Since then, we've been struggling as a group as to how to interpret GDPR. There's been a lot of gray area, and you see that in the

legal memos. We don't have clear answers in the legal memos. We keep doing back and forth. It'll be much more difficult for us to get to a policy if we don't take the input from the Data Protection Board.

I do agree with the concerns about the process and how we got here, but, that said, I am grateful that ICANN has to done this.

To address Farzaneh's concern, I actually do think that, if we get an affirmative answer, it should strongly guide our work because, if you think about it, there's a certain set of assumptions. If they say at the end of the day that this does effectively shift the liability or it's ICANN's liability, as soon as you start diverging from the principles in there, then the value of that guidance goes away. Then we're into the gray area again.

One of the things about this is that you're really getting a very powerful statement from the Data Protection Board if indeed you do get an affirmative answer. If we don't get an affirmative answer and there's a lot of ifs and buts, then I think it gives us a little more flexibility there. I would encourage this group to take an affirmative answer and work with and really try to shift our policy work to align with that. So that's how I look at this.

I do have the same concerns that Marc has about the timing because I think, Elena, you mentioned that it's mid-December when the Data Protection Board is going to meet. I just don't see how you get to a final report without knowing that answer. So I'm just replying to what Stephanie had said earlier: timewise, from my perspective, I want to see the answer. I would like to know yes or no/will it work/will it not work?

That might mean that we have to have meetings after we get the guidance, which means that we probably should not have an initial report by the end of the year.

So those were the things I wanted to raise. Thank you.

JANIS KARKLINS: Thank you, Margie. I understand that the initial report may contain only some options, that we could consider that way as well while waiting for a definite answer and then present one option only in the final report.

That said, by putting this objective for early December, we were counting the time that the community should be given for commenting on the initial report and also, following a very strong call at the beginning of the process, to be as fast as possible and bring up the considerable progress by the Montreal meeting.

Of course, all this is slightly abstract, but without an objective, we would spend probably a decade in talking about these things, and that is in no one's interest (doing that).

Alan, Mar[c], Chris, and then Thomas.

ALAN GREENBERG: Thank you very much. I don't know if James is still in the room or not. He has my permission to speak on my behalf regarding that we don't want to do this forever, we don't want to do it again, and we need to work in parallel. So those, I think, are given.

On Milton's comments about a centralized system, again, we use terms in confusing ways. In terms of what was submitted to the DPAs, I take a centralized system as a self-contained system that does all of the stuff. If we have simply a centralized entrance into a system that then gets distributed to contracted parties and things like that, I think that's relevant. That's a bit of mechanics of how the queries get submitted and not really who's doing the work. So I don't really see a conflict there.

To Farzaneh's comment about "if the DPAs say it's okay, that does not make it policy," that's true, although, as Margie pointed out, maybe we should consider it strongly. But the opposite, however, is really the crucial one. If the DPAs say it's not allowed, we'd be foolish to recommend that as policy. That's the part that we really need to lock in quickly.

I've contended a number of times that I don't believe any SSAD, no matter who says it's legal, is going to be able to be done in a single place. There are always going to be some requests which the centralized system simply does not have the information for to accept it or reject it – the kinds of requests that need to look at the other data the registrars hold. I believe there are always going to be requests that will drop through to there. If we pretend that we're going to be able to answer everything in a centralized way, I just don't see how it's ever going to be implementable. Certainly we have a strong vested interested in recommending things that're implementable.

The timing is crucial. If we come out with an interim report before the answers, it almost invariably says we're going to add another report into the process and another comment period into the process. So delaying the interim report from December may well save us time instead of making it go faster.

Lastly, regarding Elena's comments that we have 40, I think, complaints in Compliance about not releasing information, that's a very strong message to us that the policy that we put in place through the Board in Phase 1 is not working. So let's not pretend it is. Thank you.

JANIS KARKLINS: Thank you. I have now Mark, Chris, Thomas, and Stephanie. Then I would like to draw the line.

MARK SVANCAREK: I've been in the queue for a while, so a lot of what I wanted to say has already been said. I wanted to agree with Stephanie that I think the schedule is probably too optimistic – sorry – just in general and also in regard to what Margie is saying, that I think we need to this advice before we can really have a true report, and also her comments about how we got here and the history of vagueness that needs to be settled.

But really the reason that I got in the queue was to talk about some things that I guess Milton and Farzaneh had raised. Definitely, policy is generated here, and we can't assume that any feedback that any feedback that we get from any external group is going to settle the policy one way or the other. But I think there's a very good reason why

the Strawberry Team couched their proposal is a very specific way. It's not, as Milton said, that it's the only path that's possible. It's just that it's the only one we need advice on. On the other paths, we already know how they work. You have a distributed system of responsibility. All the registrars are doing their own thing independently. We know how that works. We know how to make that lawful. We don't need any advice on it.

This is the only scenario that we do need advice on. I think it did make sense for them to limit their request, their proposal, to just that one scenario. It made perfect sense to me. I don't think it's necessarily regulatory grooming or anything negative in that regard. It's the only thing we needed advice on. Therefore, it's the only thing they should have asked.

Anyway, that was my opinion. Thanks.

JANIS KARKLINS: Thank you, Mark. Chris followed by Thomas. And Stephanie is the last.

CHRIS LEWIS-EVANS: Thanks, Janis. I just wanted to quickly answer Stephanie's point. We're not asking for data that's outside of what was implemented in Phase 1. We've already detailed all the personal data items that we wanted to collect. We're not trying to get access to any other data systems or data elements that the contracted parties may have. So this phase is just for what was WHOIS data (not RDS data, as we refer to it).

It is very necessary for serious cases for law enforcement to be able to get a hold of this sort of data. It allows us to do proper due process, to avoid risks, to other data subjects, and allows us to only use the necessarily tools when absolutely necessarily. Thank you.

JANIS KARKLINS: Thank you, Chris. Thomas followed by Stephanie.

THOMAS RICKERT: Thanks very much, Janis. Following up on my earlier intervention, I still do hope to get an answer from you, Elena, on the question of legal advice – whether you had some and, if so, if you could share it.

Becky, you sort of gave an answer to my question about responsibility in that you think that we need to work on assumptions before an answer can be given. I do not agree with that. I think we've had so many different and conflicting messages from org that we can't really build anything.

Mark, to your point, we can't even work on decentralized system because ICANN plays a role. Without knowing what role ICANN is willing to accept, we can't build any system. We heard from org that, at one point, org is willing to be the sole controller for disclosure of the system. Then we heard in L.A., I think, from Goran that he's not willing to take any responsibility for disclosure. Now we see that a system where ICANN is willing to accept responsibility for a central gateway is something that ICANN is seeking advice on.

We do not need the European Data Protection Board to ICANN to say, "Yes, we're okay with accepting responsibility." Then we can flesh things out. But so far this has been a moving target.

So, Georgios, I understand that the European Data Protection Board can't give advice on specifics of a liability system because that would require further analysis. But what I do hope to get at some point is a response from ICANN to say, "Yes, we are willing to take responsibility for whatever shape or form the system is going to be." And we didn't get that commitment.

JANIS KARKLINS: Thank you, Thomas. I think, whether we do not want to hear that commitment or so, indirectly, by putting questions to data protection agencies, ICANN is showing that they're willing to take that responsibility, provided that that is fully compatible with GDPR. At least this is my reading of the document in general. Otherwise, what would be the point of asking those questions?

Stephanie?

STEPHANIE PERRIN: Thanks very much. Thomas has sharpened by pencil and put a point on what I was going to say. My first point is that the European Data Protection Board are not there to give us legal advice. That's why the good Lord made lawyers, and I'm no one of them. I'm a policy wonk and I insist on more details before I give policy advice. You have given them a bland, high-level document that they really – well, A, they're not all

lawyers to begin with, but B) I don't see how they could opine on this. So why aren't we seeking legal advice on this question instead?

Point 2 is that we have known all along that the beauty of the GDPR is that it sorts out this mutual liability that the data controllers and processors have between them. If you're not going to point out how you're going to share that liability, how you're going to transfer it, who's the controller, and who's the process, you're not going to get anything. We've been asking for that for God knows how long. I've certainly personally been asking it for six years. Whether ICANN sees itself as the controller, as far as I'm concerned, they control the contract. Therefore, they are the controller. So, really, come on, guys. We don't need to be asking the EPDP these vague questions.

Point #3 I'm going to leave until later. Thank you.

JANIS KARKLINS: In the meantime, Milton has raised his flag. If you can briefly take the floor.

MILTON MUELLER: I'm sorry to intervene again, but I just don't think my point is getting across here. People are talking to me as if I'm saying we shouldn't have asked or we don't want advice from the European Data Protection Board. My main concern is that we have been presented with false dichotomies. The statement in the Strawberry Team report is that we either have a consolidated system with ICANN being responsible for the

decision or we have no centralized system of access. That is a false dichotomy.

Think about how we might get a response to this. What happens if the Board says, "Well, possibly the responsibility could be consolidated in the centralized administrator of this system, but, under certain conditions, responsibility might be devolved down to the registrar that is the data controller." What if you get a response like that? You haven't moved the ball forward at all.

So I believe that we need to making and confronting squarely the policy decision regarding who we want to make the disclosure decision and that we have enough legal advice, both within this team and from our Byrd & Byrd and from the various documents that have been flying around from the beginning, to know what is a legally compliant system and what is not. We don't need to ask the EDPB for that. It's not like they're going to rescue us here. We have to take responsibility for designing a compliant system.

So it's fine. We'll get some advice from the EDPB. That's fine, but it doesn't solve any of our problems, really. I really resent the false dichotomies and grooming, as Stephanie put it, that's happening, where policy decisions are being struggled into this request. Then we're going to be told we have to do this because of our advice from the European Data Protection Board.

JANIS KARKLINS: Thank you. I think it would be now time to give Elena a chance to react, but before that, maybe Dan can respond to some questions.

DAN HALLORAN: Thank you, Janis. Elena, if I may, I just want to jump in on the part about legal advice and just put a caution that, in general, legal advice – it's not really clear to me … I'm responding to Thomas' questions about legal advice. You could be talking about the interactions with Byrd & Byrd. That's all fine. Those have been shared. If you're asking about interactions with DG Justice or something, Elena can talk about that kind of legal advice. If you're asking about Elena's conversations with me, that's also legal advice. We're not going to get into that. That's privileged and confidential. Just wanted to tear off that piece of it.

Also, Thomas' other question was about if ICANN is willing to be the gateway. I think that's exactly the question the EPDP has put to the Board and ICANN org and you're waiting for written responses on those. So I think you can see in the Strawberry paper that that was the hypothesis that we're working on: ICANN would operate that central gateway. But the team has put that as a direct question to the Board and org and we're working on those responses to give a direct response to the team on that. Thank you.

JANIS KARKLINS: Alan but very briefly, please.

ALAN WOODS: Thank you. One of the things that I just want to say to Elena as well is that you were talking about the end about the Compliance issue at the moment. Personally, I think this is a very interesting one. We haven't focused on it. I know Alan mentioned it. Personally to me, we keep talking about getting advice. Again, we welcome getting clarity. Who wouldn't welcome getting such clarity? But I think this is a real-world example of where it is applying, and it takes away the need for advice and goes to application. I really would love to get, as much as possible – obviously I'm sure it's a fraught situation at the moment – more detail on that because this sort of real-world example will certainly help us. So I for one would love to hear a little bit more about that if that is possible.

JANIS KARKLINS: Elena, now to you.

ELENA PLEXIDA: Thank you. I will try to cover as much as I can. Milton, you said at the beginning that, in the paper, it says that this model would remove responsibility from the contracted parties with respect to disclosure and that this is not something that the group has agreed to. Yes, you're absolutely right. This is the assumption described in the paper. We had to make an assumption to go ask questions.

It also says in the paper, indeed, that this UAM is only viable if the assumption we're making is true. Right. The UAM that is hypothesized in there is only viable if the hypothesis is true, the assumption is true.

That doesn't mean that any other model is not viable, as you said before. Another model is viable, not this model, not the unified access model, which is the most consistent model that you could have. Other models? Yes. Of course they're viable.

We have communications from the G7, the European Union, and several others. In there they describe their desired outcomes, which are around a uniform unified mechanism, the most consistent possible. This is not our desired outcome. It is their desired outcome. If this is not possible, it [inaudible] to me. They better hear it from the DPAs, not the EPDP, not ICANN org.

Where responsibility is consolidated in this system is not clear in the paper. You're absolutely right. The paper does not aim to, at this stage, of course, to see where responsibility will be consolidated between the three actors that are in the centralized system. The paper is just aimed to see whether responsibility can be consolidated in a centralized system to begin with. Then it is up to you to see if you want to follow up with it if you want to see where the responsibility will be and where you want to put it.

Stephanie, with respect to what part of the European Commission we spoke with, I think Georgios already addressed that. But just to point: we did not talk to the telecom regulators. Why would we talk to telecom regulators? They're not involved in this and they're not part of the commission, frankly. [inaudible] were DigiConnect, DigiJust, [DigiWho], and the Secretary General of the European Commission. Mostly in

particular the comments and the advice came from DigiJust who is the one who drafted the law.

Thomas, you asked about whether ICANN wants to take on the central gateway. Daniel already addressed that. There will be answers to your questions, but I would just say that Janis also made a good [resume] of it. If we are suggesting it, it means that we would be willing to, depending on the answer that we get, of course.

Joint controllership. The European Data Protection Board, as far as I recall, has said that, at first glance, we seem to be joint controllers but that needs to be looked further into. I would say this is part of what the paper is attempting to do: further looking at the controllership relationship here.

With respect to [legal] counsel, Dan addressed that. If we're talking about legal counsel overall, yes, we did take a look at from DigiJust, who gave us a lot of advice, such as to describe the processing activities that are taking place in the system – Georgios has pointed out to that – to break it down, to explain the legal basis, even if it is a hypothesis in there, so there are more and more concrete things that the DPAs can look at, even if it is a hypothesis or a question.

A very good question, [Marc], on timing. As I said at the beginning, the next plenary of the European Data Protection Board will take place on the 2nd and 3rd of December. Unfortunately, by being late with submitting the document, we are missing the plenary of November, which is the 11th and 12th. So we can hope to have something by then.

Now, that said, if we are offered by the Data Protection Board or the Belgian DPA or, most likely, the Technology Sub-Group an informal exchange, of course we will take it. But if that is not something, I can definitely say … Sorry, I'm losing my [right].

I'd like to hook on what Margie said about the gray areas. Yes, absolutely. That's the whole point around here. There are a lot of great areas around controllership with combination with the several and joint liability provision of GDPR. That is why the European Data Protection Board is coming out with guidelines about that. If it was not a gray area, they wouldn't have needed to give guidelines. That is why we have all this difficulty and you have all this difficulty. We also have a difficulty of that we cannot just proclaim ourselves something, like controllers or joint controllers.

A piece of advice that came from DigiJust to us was that, since we know that the European Data Protection Board is deliberating these guidelines, we should make points. We should draft our paper in that way so that, hopefully, when they're considering these guidelines, our situation will also be taken into consideration. That is no guarantee, but this was advice that was given to us by DigiJust.

What else? Alan, just for clarifying, there is one complaint right now with the ICANN Compliance, but the handler from the data protection authority that filed the complaint told me that she has 40+ similar ones sitting on her desk. She hasn't sent it yet over. Alan, yes, [inaudible]. This is huge to me. Just to understand, when I was originally told this

was happening, I was like, "DPA? What's this acronym?" I couldn't perceive that a DPA had filed a complaint.

This is as much as I'm cleared to share right now, but you will hear more about it over the coming days. Thank you very much.

JANIS KARKLINS: Thank you, Elena. I think, in concluding this conversation, I can say that the team has maybe a different appreciation of the substance of the document that has been submitted to the European Data Protection Board. But there is a maybe common sense of frustration on the process. I think that clearly transpired during this conversation, that we wanted to be at least notified prior to submission of the document. It did not happen. So it is regrettable but it is done, and I think we need to leave it behind us. We're hoping to receive [communication] either formal but, in a better case, informal indication that may transpire from informal interaction with the Technical Expert Group or conversations with the Belgian data protection authority, which is a handler of the question. In any case, we would expect the formal communication from ICANN org as soon as the answers are received from the Data Protection Board. That certainly would become part of our conversation here in the team.

With this, I would like to conclude this part of the conversation. And then to Stephanie.

STEPHANIE PERRIN: Just a point of order.

JANIS KARKLINS: Yes, please.

STEPHANIE PERRIN: I think it's my duty as the Chair of NCSG this year to request that, if you do have an overture from the European Data Protection Board for an informal discussion, we'd like to be there. History has shown that ICANN.org has not necessarily represented the views of the Non-Commercial Stakeholders Group. In fact, we have personally dragged the DPAs to many a meeting unsuccessfully, of course, because liability did not accrue to the same degree that it does now. But we've done it over the years, and we'd like to be there to see what they have to say. Thank you.

JANIS KARKLINS: Thank you. That is noted. At the same time, I would like again to encourage those team members who are interested in drafting additional questions to be submitted to the European Data Protection Board through the CEO of ICANN – it was invited by him – to please do so. In the conversation, no one indicated that they would do so, but still the invitation of Goran is on the table. Please feel free to use it if you wish so.

With this, I would like to conclude this part of our agenda and move to the building blocks.

ELENA PLEXIDA: Do you want to run through the operations table [inaudible]?

JANIS KARKLINS: Yeah. Building blocks. During the last meeting, we concluded a partial reading of the accreditation building block. We left on, I think, Point N. we will resume it, but before going to that, I see that staff has prepared the list of open issues that need to be addressed by the team during this meeting. I will maybe ask Marika to run us through this list. Marika?

MARIKA KONINGS: Thanks, Janis. This is a document we sent to you basically just before the start of this meeting. I know not everyone may have had a chance to open it or look at it. Basically as staff we took down all the building blocks on Thursday morning, basically after the deadline passed for everyone to provide their input on the building blocks and basically pulled out all of the open issues, questions, and comments that still remain.

[If you] just scroll down, you have an idea of the list. There are quite a list that remain in there: the accreditation building block. Just to highlight, I think Janis already flagged that as well. There are a couple of outstanding action items that people were assigned on Tuesday that we don't have language for yet. I do think we have an upcoming coffee break, so it'll be really helpful if people can do that homework so we can discuss those items. As I said, you can scroll through. It gives you an idea of at least what we expect the focus to be for the discussions for

each of the building blocks throughout today and the upcoming meetings.

It is a fairly long list, but at the same time, a lot of people have made good suggestions or just specific wording that has been proposed. So we hope that this will help focus on the open issues where comments have been made instead of starting at all the building blocks from zero. So that's something we just wanted to share before we, I think, dive into accreditation again.

JANIS KARKLINS: Thank you. As I mentioned, my suggestion would be that we really focus these four meetings here in Montreal on those outstanding issues. Then the text will be consolidated and then put together in the draft initial report that we could then examine. We'll do a reading of the report as a whole to look for inconsistencies because it may happen that some building blocks may not be fully aligned with others, since we are working on them separately. So that's my suggestion.

Accreditation. Can we get it up on the screen. I asked staff also to send the link to the mailing list or to the Zoom chat so that those who prefer to work on their own computer screens can do so.

[inaudible]

MARIKA KONINGS: Yeah. We're just having one slight challenge because the version we're sharing is the View Only one, which means people cannot see the

comments that are added because those are only viewable by those with editing rights. So we're just figuring out how to share that with you.

UNIDENTIFIED FEMALE: [I need to share my screen].

MARIKA KONINGS: Okay.

JANIS KARKLINS: Also, some team members in the Zoom chatroom suggested that maybe we should switch to the Zoom also for the speaking order. I don't mind. Either way. So if you prefer Zoom to establish the line of speakers, that's fine with me. I see it here on my mobile phone. Then let's move to the Zoom room and see whether that works better than people raising a name plate.

In the previous session, we went through the working definitions. I think that we reached more or less a common understanding on those working definitions. I see that there is a third bullet point on accreditation, and that needs to be …

MARIKA KONINGS: You want me to speak to that one?

JANIS KARKLINS: Yes, please.

MARIKA KONINGS: Thanks. This is the first issue we identified in the list. This was originally listed as a TBD: the accreditation authority auditor definition. Staff has gone ahead and put in a definition there that's of similar style as some of the others and that we hope confirms to what the auditor is expected to do. Of course, if there are any concerns about this, it's open for input.

JANIS KARKLINS: Thank you. Any comments on the working definition of the accreditation authority auditor: an independent entity that is contracted by ICANN org to carry out auditing requirements as outlined in the auditing building block. Can we agree on that?

Body language says yes. So no requests for the floor. Then the rest of the working definitions I think we stabilized.

MARIKA KONINGS: Do you want me to comment on [inaudible]?

JANIS KARKLINS: I can put it on the screen.

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: Yeah.

MARIKA KONINGS: The next item on the list is to review the updates that were made by Alex to update references to framework. I think you see that here if you scroll a little bit down, Caitlin: basically the change has been made. Instead of referring to framework, it's referring to policy. I think that the description I'm trying to see there in Bullet C also aligns with the description of what it actually means. This hopefully aligns with what was discussed and clarified on Tuesday's meeting. So I think this is basically the change: from framework to policy and the updated language that's in Bullet C that you see here on the screen.

JANIS KARKLINS: Thank you. Let me see with the suggested change in the chapeau sentence. "The following principles under [inaudible] [accreditation] policy, not framework. So then we get that the accreditation defines a single accreditation authority, run and managed by ICANN org. This accreditation authority may work with external or a third-part identity providers that could serve as a clearinghouse and verify the identity and authorization information associated with those requesting accreditation."

So that is Bullet Point C. Can we accept that change/clarification?

Brian?

BRIAN KING: Thanks, Janis.

JANIS KARKLINS: You don't need to do double-booking. The zoom room is enough.

BRIAN KING: I have a lot to say – no, I don't actually. Can we put Alex's comment in a footnote? I think it just helps to clarify what "run" and "managed" means there.

JANIS KARKLINS: Alex's footnote: "Note that ICANN org may outsource this function to a qualified third party. However, the details of this are outside the scope of this document." So that's the footnote that is requested. Would that be okay?

So it seems to me. Then I take it that C is stabilized, so let us now move to F, whereas, again, the proposed edit is now seen on the screen. Marika, please?

MARIKA KONINGS: Thanks, Janis. On this specific one, there's some edits that Alex provided here in response to the comments that were received during the last call. But here's also an outstanding action item for the registrar team: to review this list in line with – I don't remember which document we provided in the notes. I see Matt nodding. I don't know if that means that they're okay with it or they still need to review.

MATT: Thanks, Marika. It was to look at the Registrar Stakeholder Group document under the current temp spec about data registrars wanted to receive. And, yes, we reviewed it. It's all included here. Thanks.

JANIS KARKLINS: So that means we can remove all brackets and we can put this list as it is drafted in the document. Thank you. That's noted.

Any objections to that?

I see none, so let us move then to the next item. That is N. We discussed that we would split the text on de-accreditation. This is de-accreditation. Now we changed it to [revocation in] two: one related to users of SSAD and then another related to the accreditation authority. Now the proposal is now on the screen. The [revocation] policy for individuals/entities should … Marika?

MARIKA KONINGS: Sorry, Janis. This is actually not updated language. This is an action item that Margie and Volker had: to work on proposed updated language. I don't think we received anything yet. So they may have something to do in the coffee break.

JANIS KARKLINS: Sorry. I was too fast. Margie?

Oh, okay. Then we will revisit it immediately after our coffee break with the proposal from Margie and Volker.

Let us move to Q.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: Yes, please.

MARIKA KONINGS: Thanks, Janis. This is one where I think James has provided language. I believe it's the last sentence that has been added – again, in line with the discussions on Tuesday's meeting. So the group should review if this appropriately reflected the discussion and whether the whole text can be accepted as is.

I do note that there's still some bracket language in the first part. "De-accreditation may occur if it has been determined (or if ICANN determines)." So that may be another one where the group needs to confirm if they believe they can already confirm at this stage which one it should be.

JANIS KARKLINS: Thank you. Let me then open the floor for this conversation of Sub-Point Q, which is now on the screen.

I have three hands up. Brian, Hadia, and James, in that order.

BRIAN: Thanks, Janis. I think Q looks good and should probably track N since it's going to be pretty similar, I think. If that last sentence is the one that James added, I think that looks good, too. Thanks.

JANIS KARKLINS: Thank you. The question on "De-accreditation will occur if (then options) if it has been determined (or ICANN determines)." Any idea from your side?

BRIAN: Yeah. Thanks, Janis. I think it's better if it's then passive "has been determined" because we're not certain that ICANN is going to do it. Thanks.

JANIS KARKLINS: Thank you. I'm just collecting preferences. Thank you, Brian. You can put your hand down. Hadia?

HADIA ELMINIAWI: To me, Q looks good as well. But the only thing that we did not address here that maybe we do somewhere else – I don't know – is what happens to the accredited users. This is an important, I think, issue that we need to tackle because, if we de-accredit the accreditation authority, then, by default, every accredited user will be de-accredited as well, and then we won't have a system or users. Thank you.

JANIS KARKLINS: If the group is in agreement on what Hadia just said, can I ask Hadia to propose language/a sentence?

JAMES: Actually …

JANIS KARKLINS: Yes, James?

JAMES: If I may respond to Hadia, the last sentence is an effort to address that specific topic: the nature or the circumstances leading to the accreditation could cause it to revoke some or all of the outstanding credentials. I think I tried to leave that specifically flexible because, if it were something not related to the accreditation or the authentication validation or vetting process, then it would allow those outstanding credentials to remain operative.

But if the nature of the accreditation was that the process used by the authority was flawed, then those would have to be revoked. I think the analog we keep going back to is the SSL certificate authority, where sometimes, if there's a problem with an SSL certificate authority, they will revoke certain certificates – not all of them, maybe a portion of them, maybe all affected.

So I think that's what we're trying to capture in a somewhat vague but deliberately flexible sentence at the end.

HADIA ELMINIAWI: I agree and I understood actually what you put in here, but still, what happens if all of its [outstanding] credentials are revoked? What happens then? I think maybe we don't need to address this here, but we need to think about that. and put a clause in the policy that addresses such a situation.

JAMES: Okay. I'd be happy to add a sentence or something that says essentially that, if a user's credentials are revoked, they would reapply for recredentialing, or they would essentially become an uncredentialed user.

HADIA ELMINIAWI: Because if this happens and none of the users can actually access the system, then meanwhile maybe we should think of another process or another way for which requests can go until another maybe authority is in place. I don't know. I'm just trying to think. What's the path until we have another system in place. I see the logic behind what you put here, and I agree with it. I'm just thinking, what will happen until we have another process in place? Would they go directly to the registrars and registries? We just need to think of something, a path. Or it will be on hold for whatever time we need to set another system in place.

JAMES: I disagree and I think that that is not our problem to solve. They become unaccredited like all the other universe of unaccredited users. They can reapply or they could—

HADIA ELMINIAWI: To who? Because you de-accredited the accreditation authority. So, even with reapplying, who would you apply to?

JANIS KARKLINS: Let me suggest. I recall that somebody called the de-accreditation of an accreditation authority as a nuclear option. So let's focus on the, let's say, 99% of probably situations and develop policy based on common sense and leave those extreme unlikely cases either completely outside of our scope or at the very end when we will accomplish building the system, which is most probable. So that would be my suggestion.

Milton, you had your hand up.

MILTON MUELLER: Pretty much what you just said. I agree with the way James has handled this. I think that, if an accreditation authority has proven so bad that we have to withdraw them, then that's a big problem. But that's a well-earned problem, shall we say. We'll just have to come up with another accreditation mechanism. That's just too bad for the people that were abusing the system.

JANIS KARKLINS: Thank you. Let me remind that we're using Zoom for the speaking order. I see Margie and Alan's flags up. Please, Margie and Alan. Then I would like to close this conversation.

MARGIE MILAM: Hi. This to me sounds very similar to what happens when a registrar becomes de-accredited. We have a process for that. Many of you were around at that time. Originally ICANN didn't have a process for it and it was complete chaos. I think it was RegisterFly when it was de-accredited. ICANN had to come up with something very quickly. I don't think it was a good thing to not have that be addressed. There's a difference between an accreditation authority not doing what it needs to do and actually someone that's accredited. So I would think that we would want to come up with some sort of policy on transition, finding a replacement accreditation authority.

I'll give an example. If it's trademark professionals or cybersecurity professionals, there may only be one accreditation authority. To say that entire group of folks do not have access because one accreditor agreement was terminated would be a problem.

So I would encourage this group to look at what we do for a registrar de-accreditation and follow a similar approach.

JANIS KARKLINS: Thank you. Alan?

ALAN GREENBERG: Thank you very much. The real problem here is that there are many registrars and, although we obviously know they're not created equal, they all have the same legal ability to do things and we can transfer things from one registrar to another. We're not likely to have multiple accreditation groups existing an operating in parallel for the same class of user or whatever it is, whoever it is, they accredit.

So I tend to agree that, if we ever come to this kind of situation, we're going to have to de-accredit carefully and think about the transition. We can't just pull the plug and say, "Oops, not our problem." I think it will be our problem, but I'm not sure we can plan ahead for that kind of eventuality, certainly not until this whole thing is a lot firmer. Then we could perhaps, as we get closer to the end, start thinking about what would happen if. But I think that's way off of our plate right now.

JANIS KARKLINS: Thank you. Stephanie [inaudible]?

STEPHANIE PERRIN: Thank you. "Surely," said the optimist, "there will be audit of these accreditation authorities." Therefore, we will be getting a clue as to the reliability of the authorities. Plan B can start being developed as soon as we have experience. So I'm not sure. To me, this is an implementation issue that should be deferred, but I'd just like to put that marker in that, if we have the appropriate controls in place, it's going to be much less of a theoretical problem.

JANIS KARKLINS: Thank you. Thomas, Mar[c], and Alex.

THOMAS RICKERT: We do have the language of graduated penalties in there, so we have proportionality built into the current language. Just to illustrate this, if we find out that an accreditation authority is selling accreditations to people that shouldn't get any, then I think it would be perfectly justified to suspend the accreditations of all accredited requesters until the thing has been sorted. Well, if there is an issue with the accreditation authority itself, not having five papers to ICANN in time, that does not suggest there's something wrong with the accreditations themselves. Then you wouldn't touch the accreditations themselves.

So I think, if we have graduated in there, maybe we lose the often word "proportionate" because the principle of proportionality is often used in legal context so that the implementation folks do know what we mean with this.

JANIS KARKLINS: Thank you. Marc Anderson and then Alex and then coffee break.

MARC ANDERSON: Thanks, Janis. Now I feel pressure standing between us and the coffee break. I think Thomas pointed out nicely that getting to a situation where we have to suspend the accreditation authority is pretty significant. There are graduated penalties in there. I think that's well taken into account.

But I also wanted to point out that a couple of the interventions I heard seem to indicate that people thought there'd be multiple accreditation authorities.

Marika, could you scroll up to C for a second? Or Caitlin, sorry. Just to clarify, the language in C that we just reviewed and agreed to is that there'll be a single accreditation authority and that an accreditation authority may work with external or third-party identity providers to serve as clearinghouses. I raised my hand because I want to make sure we're all on the same page and understand what the language is we've all agreed to so far. We've agreed to a single accreditation authority which may use multiple third parties to serve as clearinghouses for identity providers because, based on the interventions I was hearing, I'm not sure we're all on the same page on this point. Thank you.

JANIS KARKLINS: I think we are. Alex?

ALEX DEACON: Thanks. I was going to say the same thing. We should be careful about the terminology we use. We have decided that we're going to have a single accreditation authority run by ICANN and they will have one or more identity providers.

So, as we have these discussions, we should be mindful of the definitions and using the right terms. Just agreeing with what Marc said.

JANIS KARKLINS: Thank you. Let me then suggest the following. On Q, we would delete "ICANN determines" and would leave it as "it has been determined." We would accept the last sentence, which is suggested by James, and we would stabilize this paragraph.

If I may ask, James, since you're the penholder on this, if you could think of the part of the discussion we had on what happens if a nuclear explosion happens and how we would proceed. If you could try to formulate in one sentence something for consideration of the group after the break.

In the meantime, those who have homework during the coffee break, I encourage you to do so. With this, we're breaking for ten minutes and reconvening at 10:30-ish. Thank you.

Okay, shall we start? If I may ask team members to take their seats. Let me then go back now to Sub-Point N. That was outstanding. I understand that there is a proposal on the table that was crafted by Margie and Volker. The text, as it is, now I displayed on the screen. If somebody can read it, since I cannot see on the screen.

Caitlin?

CAITLIN TUBERGEN: Thank you, Janis. If you look at the bottom of Sub-Point N in brackets, the text appears in green. This is text that Volker and Margie came up with the idea to recount for a situation where someone within a very

large organization may have abused the system but that may not implicate the entire organization. However, in the event that there's a pattern of abusive behavior from within an organization, the organization's credential could be suspended or revoked as part of a graduated sanction.

The language reads, "In the event there is a pattern or practice of abusive behavior within an organization, the credential for the organization could be suspended or revoked as part of a graduated sanction."

JANIS KARKLINS: Thank you very much. Now, a question to the team. Can we accept the language in its entirety (the one that's in yellow) and then the additional sentence that was proposed by Margie and Volker? Any comments?

So I understand that that is something we can live with? Good. It turns green then.

I also understand that James has come up with one additional suggestion to de-accreditation of an accreditation authority. Now it is on the screen. Caitlin, if you could read it again.

CAITLIN TUBERGEN: Thank you, Janis. You'll notice again in the green text something that James had suggested in the chat. Now the sentence reads, "Depending upon the nature and circumstances leading to the de-accreditation of

an accreditation authority, some or all of its outstanding credentials may be revoked or transitioned to a different accreditation authority." That accounts for the issue that, in the event that the accreditation authority is de-accredited, those credentials could potentially be transitioned to a new or different authority.

JANIS KARKLINS: Thank you very much. James?

JAMES: Thanks. I wanted to just make a couple of comments on this. Hopefully this addresses the concerns that were raised about what happens to those folks who are left holding worthless credentials. Those of you who went to ICANN Hyderabad remember we were all holding a lot of demonetized money. I think we are all familiar with that feeling.

But I just want to point out that this is now somewhat inconsistent with, I believe, Sub-Bullet C, which essentially said that there will be one and only one accreditation authority. So where did this new accreditation authority come from? Did it fall from the sky? And how is it ready to accept all these?

But I think we can try to address that or we can acknowledge that this is allowing some flexibility in the implementation. While the path for any particular or given credential authority or credential holder is maybe not certain, at least we have a policy that is flexible enough to deal with all potential scenarios and situations. We should allow it to remain flexible rather than try to continue to – I think I put this in the

chat as well – design a policy for mechanisms for when that policy fails. There is no end to that work. We will be here forever. So I think at some point we need to say it's a safety net and it's there and it's not perfect but we can move on.

JANIS KARKLINS: Thank you, James. Let me collect some reactions. I have Alan, Alan Woods, Chris, Brian, and Matthew in the line.

ALAN GREENBERG: Thank you very much. I don't think that is acceptable right now because in C we say there is one accreditation and then, in Q, you were saying, if one accreditation is de-accredited – we already said the de-accreditation group is ICANN – then the concept of ICANN de-accrediting itself I just don't think makes any sense.

Now, if we change Q to say, "If there are sub-accreditation groups," units or whatever title we want to put on them, "then they may be de-accredited and transition to another one or be replaced." But as long as we're saying there is only one accreditation authority and it is ICANN, the whole concept of who's de-accrediting it doesn't make any sense at all.

So I think we either have to strike Q all together or assume that there are some sub-units under ICANN which might be de-accredited. I don't see how we can live with two that just don't fit together at all.

JANIS KARKLINS: Thank you, Alan. Alan Woods now?

ALAN WOODS: Thank you. Apologies. This is actually relating to the last one. It's a very quick one because I didn't get my hand up quickly enough in the last one. In relation to the additional Volker and Margie language, you talk about an organization, but earlier in N you talk about entities. So we should probably keep that consistent and make it about entities, not organizations.

JANIS KARKLINS: Yeah. Thank you. Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. We were discussing in the coffee break another thing Alan just brought up: the whole issue about how there's other entities underneath accreditation authorities that may cause problems to get the accreditation authority de-accredited.

What I would propose that we do is maybe add another section here – de-accreditation of the identity providers – because that's the level that we're probably more looking at. The language could be pretty much the same, but just change accreditation authority for identity providers. And then a change to the new language that was suggested is, rather than "different," it would have to be "new" because there is only one accreditation authority. So it would have to be "new" rather than "different." Thank you.

JANIS KARKLINS: Thank you, Chris. Brian?

ALEX DEACON: Hi, it's Alex. I'm going to take Brian's spot. I was going to say the same thing. I think it doesn't make sense that– I'm agreeing with Alan Greenberg – if we have a single accreditation authority and it's run and managed by ICANN, that would ever disappear. I think it makes more sense to perhaps focus on their use of these identity providers and ensure there's a mechanism to de-accredit them when things go awry. Thanks.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: I think we're harmonizing here. I think it might be helpful to point out that the whole notion of de-accreditation emerged from earlier conversations coming from Alex in which we were assuming there would be a bunch of self-nominated accreditation agencies and we needed to make sure that they were not fly-by-night operations that were accrediting anybody.

If indeed the accreditation authority is essentially ICANN, then we don't need de-accreditation, per se. We need to keep ICANN accountable in who it uses as the identity providers. I think we need to focus more on

the de-accreditation or de-authorization of users rather than the actual accreditation process itself.

My question for the lawyers in the room is whether, under the GDPR, ICANN could be held for accrediting people and not properly auditing them as a breach of data protection rights, and would that be a suitable accountability mechanism for keeping ICANN's accreditation process in check?

JANIS KARKLINS: Thank you, Milton. [inaudible] question as well. James, your hand is up?

JAMES: I just want to agree with Chris' proposed edits. It seems like it harmonizes Q and N, and that's what we were trying to do. We were working in two different directions and it brings the two paths back together. Thanks.

JANIS KARKLINS: Thanks. In light of this conversation, James, could you try to put this together?

JAMES: Yeah. Chris is raising his hand and I would begrudgingly go ahead and let this take this action item. Thank you.

JANIS KARKLINS: Okay. Then, Chris, you have been pointed to. If you could send your proposal to either Marika or Caitlin, then we would, once it I ready, put it on the screen.

Let me go to the next … So we would leave for the moment Q, so we would go to Sub-Point T. I understand that there may be a need for further conceptual conversation on this point we started. It seems that there is a slight divergence of opinion. So let me engage now on this notion of limitations of in terms of numbers of requests send by SSAD.

I have James first.

JAMES: Thanks. Just to let everyone know, it's not that we didn't do our homework. It's that Greg and I couldn't finish our homework in time. I think that's probably a better characterization.

The concern here, I think, from my perspective – then I would invite Greg to give an alternative perspective – is this looks like a blanket prohibition. It reads like a blanket prohibition on any restriction of legitimate requests by accredited users, except where they present a threat to the SSAD. I think that that is good, but it is a little too narrow. There are situations operationally where legitimate requests would need to be restricted or regulated. This is something that we saw with the old WHOIS system. This is something that we see with SRS systems that are handling registrations or updates to existing domain name registrations. This is just a part of our industry. It is not realistic to say

that something will be unlimited and also perform under an SLA at all times. It has to have some boundaries and some guidelines.

The example that I give – we have people from GoDaddy that are much smarter than me in the room – is, if a portfolio holder that has, for example, 5,000 domain names with GoDaddy decided to change their e-mail address and they send through a batch of 5,000 e-mail change transactions that we have to now send to all the different registries, it is fair that my change, my request, my new registration should have to wait in line behind all of that and wait for that practice? So we will essentially say, "Well, let's take them in batches. Let's say 10,000 every minute until we get through this large batch." But that leaves room for other users of the system to have access under the SLA.

I raise this because I think there is a concern that there will be some users of SSAD that use this system use this system very heavily and process large numbers, and then there will be some users that maybe have a one-off, depending on a particular investigation, a domain at a time.

So what I proposed was some language that included the words or the phrase "demonstrable threat to the SSAD or to protect equitable access by all users." I understand that that was considered too restrictive by Greg. I don't want to mischaracterize, but I think that was the gist of it.

I think the one thing that Greg and I did agree on was that perhaps this sub-bullet doesn't belong here. It may in fact be more appropriately moved to the part where we talk about access policies and some of the

things that we've characterized as abusive use of SSAD. So maybe it belongs more appropriately with those bullet points.

That was where we left it when we got on the planes, so that's probably where the conversation should start.

JANIS KARKLINS: Thank you. Greg, do you want to give your perspective?

GREG AARON: Yes. I think we're all in agreement that we have to protect the system from what we could call illegitimate queries that shouldn't be made. Now, this system, by definition, is going to one that is controlled. It is not like the Wild West of anonymous, open RDS services right now. The users will be known. They will be logged. They will get kicked out if they're making an illegitimate request. So this is a different situation.

Now, what we don't want to lose sight of, I think, is the idea that this system is designed to serve legitimate queries and that sometimes those queries will come in numbers and with frequency. We do have a situation right now in open WHOIS and RDAP access where various contracted parties had different ways of dealing with this and they imposed rate limits. You can read about that in SAC 101. Some of those limits are extremely low. For example, there's some providers right now who will only allow one query per minute, which does not fit the need of the SSAD system we are talking about. The SSAD system does need to provide performance better than that. The question is, how do we define that?

From the other side, we want the system to do what it is supposed to do. Talking about queuing and batching in some ways is an implementation issue, perhaps. I'd like to see us come to sort of language that acknowledges what the system is generally designed to do and make sure that queries can be made to fulfill the needs of the users, which will include security purposes.

So we don't have that language yet. In some ways it's down in implementation details. I'd like, basically, a policy or what we'd call a business requirement that the system needs to have some sort of performance metrics. If ICANN is going to run this centralized system, it would be responsible for designing and meeting those. Then there are ways to figure out how to serve the queries back and log them and so forth. So that's the concern.

I think we need to come up with that kind of a general language that the system has to be designed and be provisioned to deal with the load it's going to get. Thanks.

JANIS KARKLINS: Thank you. Let me take a few other reactions. Volker followed by Margie.

VOLKER GREIMANN: Thank you. I'd like to come back on something that Greg said. He said very rightly that currently WHOIS – or in the past – had no … SLA had no response time requirements, other than that the response must be provided in a certain time. Yes, but rate limits were perfectly fine. Now

you're proposing a system that is arguably more complicated and requires more manual review and more labor on the part of the disclosing party to get rid of those limits that have been in place for decades in the WHOIS environment for whatever reason.

I think that there needs to be the ability for the disclosing parties to limit access for the reasons that James enumerated and for various other reasons that have led to certain limitations to access to current WHOIS. Those reasons are valid in the new environment for the new systems, just as they have been for WHOIS as well.

So we should be cognizant of the abilities of the disclosing parties to provide that service on the one hand and also of the history of the WHOIS system that had limitations that were not in any PDP or [turned] by ICANN.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I think I'm confused because, even if there's someone that's looking up thousands of records, it still boils down to an individual RDAP request per record, right? So I guess I don't understand why this becomes an issue. If the centralized authority, like ICANN, receives a request for 5,000 lookups, then it's going to have 5,000 individual queries that go to the various parties. And the contracted parties, under the assumptions that were in the paper, won't even know where it's coming

from because all they're doing is responding to ICANN's request. They don't see the requester. They don't see anything.

So I think that we're confusing concepts here. It seems to me that that would just be a first-come-first-serve system. Greg, is my understanding correct, or is that not really correct?

Okay. Please clarify so I understand what we're talking about here then. Thank you.

JANIS KARKLINS: Thank you, Margie. Greg?

GREG AARON: There's some parallels with WHOIS right now. First, let's clarify that, if queries come in, this centralized system has to then receive them and distribute them.

Then, the amount of time it takes for the contracted party to consider that query is a whole other issue that we're not talking about quite yet because in some cases they'll have to do a balancing test and so forth.

RDAP and other things that we're used to are query response things. Basically, it's a matter of provisioning. Let's say a registry system has to have the ability under SLAs to receive the queries and respond to them within a certain period of time, which is within milliseconds. Now, there is decision-making underneath that, but that's a query and response and you have to provide the response back.

A registry system is also generally supposed to be provisioned in order to handle those queries. They do get excess queries sometimes, sitting around sales, for example, where there might be more demand. The registry systems are supposed to be provisioned in order to handle that. What I'm saying here is, whatever the system is, be provisioned for the load because there will be frequency and there will be volume of requests.

Beneath that layer are the contracted parties. Then they also are going to have some capacity to receive those queries and then, eventually at some point, send a query back.

So there are two layers that we have to think about here. There need to be SLAs for the burger meat in the middle, which is a central system. Then the contracted parties have to have the ability to handle queries related to their domain names. They're getting queries for those domain names for some reason, which is a good reason, in this system. By definition, the queries are coming in for good reasons.

So this is a matter of provisioning in a lot of ways. Rate limiting in some ways by the contracted parties is a way to manage their provisioning. What we're saying, though, is that some contracted parties put such a low level of query access on people for one reason or another. People can't get data. Period. That's the problem.

JANIS KARKLINS: Then the question is the text on the screen, which suggests that the accredited organizations or individuals will not be restricted in the

number of requests submitted at the time, except then there is a demonstrable threat to SSAD. So who had a problem with this formulation? Is it the contracted parties or is the … The contracted parties have that problem. Okay.

James, you're next in the queue.

JAMES: Exactly. I just want to point out something Greg said earlier. He said this is an implementation issue, and I agree completely. This is a very complicated implementation issue. What we have in the policy right now – this sentence reads as nearly a blanket prohibition against any kinds of restriction of legitimate traffic, which is constraining to the implementation and doesn't allow for those thoughtful discussions. It essentially says, if I have accreditation and I'm not abusing the system, you can't restrict or limit my access. I think that is too restrictive, too constraining, for the implementation.

I think we have a number of real-world examples where even legitimate users are contending with each other, not abusive traffic. They're just all trying to drink from the same water fountain at the same time and it's just not possible. So allowing some orderly queue could be interpreted for some as a restriction.

I think what I hear Greg saying and what I hear others saying is that some of the concern is that some of contracted parties in the past have used this as a means to effectively cut off access at all. So we can use words like "reasonable," or, "practical," or, "proportional," or whatever

we need to do to prevent that kind of bad behavior. I think it's bad-faith behavior. We can call it that. But I think we can't just say that you can't restrict it at all. That is not the world we operate in. Thank you.

JANIS KARKLINS: Thanks. That's clear. Let me take those who have no spoken yet. Mark Sv, then Brian, and then Thomas.

MARK SVANCAREK: This language is perfectly fine because this is about how many requests you can make. What James is talking about is fulfilment of SLA, and those are different.

If I need 1,000 records and there's other people in the queue before me, that's a scheduling issue. Whoever is doing the scheduling, whether it's the contracted party themselves or whether it' the central authority, knows who's making the requests and they can schedule round robin. They could fill the queue however they want.

This says "shall not be restricted in the number of requests that can be submitted." That's the important thing for this section. How many times can I request? I am not restricted. What is the SLA for having those requests fulfilled? That's the operational issue. That's what goes in the other section. In this section, we're just talking about how requests you can make and it will not be restricted unless you're a demonstrable threat. All this other stuff is about SLAs. We'll talk about that later.

So it's talking about that I'm blocked in the queue because somebody makes more requests. Well, that's a scheduling issue and that's a well-known problem in computer science. Long backlogs and stuff like that? That's a scheduling issue. SLA fulfillment. This is just limited to the number of requests I can make.

"Will not be restricted unless it poses a demonstrable threat to the SSAD." So I think this language is perfectly good and it belongs in this section. But there does need to be a further breakdown of how SLA is resolved in the other section. Thank you.

JANIS KARKLINS: Thank you. Brian?

BRIAN: Thanks, Janis. I think Mark made a good point that I was hoping to make in that perhaps it's worth noting here then that ICANN is and will negotiate with contracted parties on RDAP SLAs. I think, as to the system, this language is fine because this doesn't mean that any of these requests are even going to go to a contracted party but that, if the requests do, then that'll be handled by the contract negotiation that are about to start between ICANN and the contracted parties over the RDAP SLAs. Thanks.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: I'm not sure whether we really need this language here. I think we're discussing two different things. What we want to prevent is people DDoSing the system. That would be a threat to the system. We can put language here or elsewhere that you mustn't do that, you mustn't put the system under pressure so that it might break down.

With respect to the number of queries, I think we have the required safeguards elsewhere. We say that it's limited to legitimate requests, that you only get the data that you need to get to fulfill the purpose of the request. If you are, let's say, extremely busy as a company and if you find 10,000 domain names that have been registered that are identical not just to the trademarks that you own, then nothing should prevent you from issuing disclosure requests for those 10,000 things.

So I think the answer is elsewhere. As long as you have the need for the data, as long as you have the legal basis for doing the request and all the other things, I think we can't possibly find language here that will prevent the system from being abused.

JANIS KARKLINS: If we would, in the first line, before "requests," put "legitimate," would that help contracted parties?

No. Okay. Volker?

VOLKER GREIMANN: Two points, the first point being I think limiting the demonstrable threat to the SSAD alone is too narrow. It would have to be to the SSAD and

any parties providing services within the SSAD or working in that concert because, if the SSAD itself is fine but any one part of it is overloaded that is providing part of that service, then that would also probably be a problem.

The second part is that I still would like to reiterate that we are proposing a limitation that has not been there in the WHOIS. WHOIS access has been legitimately restricted in the past to a number of request per minute or per hour or what have you, depending on the setup of the different parties. This now proposes restriction on a perfectly fine, perfectly legal (in the context of ICANN), policy practice. We should be very cautious about putting in new restriction that has not been there before.

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: Not weighing on this specifically, but an important form of background information is that what you're talking about, again, is contention and limits. The miracle of the price system is a very good way of dealing with this. So, if we're talking about free requests, we're going to have serious problems of the sort that you're now debating. If there is in fact even a miniscule price for these requests, then a lot of these problems will not happen. People will rationally calculate how much it's worth to them to have these things, and they will not overload the system. But if it's free, you're going to have these problems.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. We started off this morning talking about whether it might be possible for ICANN to assume all responsibility and offload this from the registrars. Now, there are some people who believe that's not possible. We're asking the question.

I would propose that the answers to what we're discussing right now may be very different if we end up implementing a system like that. Clearly, if every request goes to manual intervention by a contracted party person, by a registrar or a registry, it' a different environment than if many of the requests, and certainly the high-volume ones, may be made in an almost completely automated way. Clearly, ICANN is not going to employee 10,000 people looking at requests.

So this discussion is an important one, but I'm not sure we can have the definitive answer until we know how the system is going to be built and who's going to be actually making the decisions. Thank you.

JANIS KARKLINS: Thank you, Alan. James?

JAMES: Thanks. I'm actually going to agree with Alan that this is something that we need to understand better. It is dependent upon SLAs that we

haven't talked about or written yet and we just assume will be there. I think that that's one of the reasons why having a blanket prohibition in the policy is concerning, whether it say it's rate limiting. Another example: You mentioned automated systems, Alan. This could be a captcha in front of a request. Would that be a restriction that would be prohibited by this policy, potentially?

But I actually wanted to go back. It wasn't what I was originally got in the queue for. Milton's intervention about the pricing got me thinking that perhaps the solution to this is to create some sort of a peak pricing per transaction or dynamic or flexible transaction fee, similar to what you see when you try to order an Uber when it's raining. If there are a lot of people trying to get a car or trying to use the same resource at the same time but the resource is finite, how does it fill those requests? It raises the prices. Some people see that and they say, "Well, you know what? I'll just get my umbrella and walk," and some people say, "I'm going to pay the extra price and get then Uber."

So I think that is actually an interesting way of perhaps solving this problem, but again, this particular line, this sentence – you asked if we were okay if we added "legitimate." I think "legitimate" is covered by the last bit. We're talking about legitimate traffic. Illegitimate traffic is already bad and we're now talking about contention between legitimate users. So I think that's one possible approach: let's go with the dynamic pricing on those per-transaction fees that we also have not discussed yet.

JANIS KARKLINS: Thank you. Let me take two more and then we'll see what we can do. Let me take Mark Sv and Stephanie.

MARK SVANCAREK: I wanted to build on the interventions of some other people. I want to build on something that Milton said about the costs. James touched on it as well. I think we can't talk about costs without talking about SLAs, and we can't talk about SLAs without talking about costs. So, to the extent that we're talking about either of those things, it's in a different section, as I said before.

I disagree with Milton that, even with cost, there won't be contention. As James said a moment ago, there could be multiple people doing multiple investigations all at the same time. It's legitimate. You will might wind up with contention. I don't think I like the dynamic pricing concept, but let's talk about that in the SLA and cost recovery section.

I agree with Alan G. that, since we are building on some speculation here, there's going to need to be some iteration. We just need to keep that in mind as go through this process, that we won't get 100% in the first pass. We will have to iterate.

Finally, James, I still think that this language is not a blanket prohibition on certain implementations by then contracted parties. This is just relate to the rate of requests, not the SLA fulfillment. So I really want to make a distinction between those two things. I'm not advocating a blanket prohibition on the contracted parties. I don't think this language does either. Thank you.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Thank you. I'm way back at something that Margie had said that causes me some concern. Maybe I missed something. I [haven't] been paying attention lately. I can't see any justification for these RDAP request being anonymous. In other words, yes, it's another RDAP request, but the requester has to be identified. One of the reasons to do that is that there will be local information about protecting, for instance, human rights defenders. A cautious human rights defender who's aggravating a particular country is going to make sure they establish their registration and their website in a country where they have constitutional protection – e.g., Canada. I'd do it here. I'd do it in Montreal and I'd make my data didn't cross borders.

So I would be loath to see ICANN as the accredited accreditation authority yanking in any special data that they need to determine whether a request should be granted or not. I would put a caveat on my data and hope that that caveat would be instructive in the event of a request. Thank you.

JANIS KARKLINS: Thank you very much. Thinking about a possible way forward, I will say something that maybe I will ask Greg and James to respond. Actually, we're talking about that that system may have some limited capacities in response because of the technical limitations. Would simply the

addition at the end of the first part of the sentence "will not be restricted in numbers of the legitimate requests that can be submitted at the time with the understanding that the possible limitations in response capacity and speed of the system, except where accredited organizations pose the most [credible] threat." … So we're saying that, if there's enough legitimate requests, we understand that there are maybe some limitations in speed of dealing with them, and that is how we determine this principle. Then, of course, in implementation, we add things in terms of what then system should be and what should be the technical characteristics of the system.

Greg?

GREG AARON: I've proposed some language to James which would go in the SLA building block, which I think is G, which I think might be the better place for some of this stuff, which would talk about some high-level principles, one of which is: whoever builds this system needs to provision it to a certain level, etc.

So we have some proposed language between us that would go in that section that I think would get at some of these issues. We could work at that offline because we haven't gotten to G yet. I don't know how we're going to leave T right now. What's your proposal again?

JANIS KARKLINS: I was simply proposing to add, after "at the time," wording of "with the understanding the possible limitations of response capacity and speed

of the system." So that would accommodate the interests of those who may have many legitimate request and accommodate potential limitations of the system in terms of response time, response speed. So I'm just trying to accommodate what I understand is an issue.

James, would that go in the direction of mitigating your concerns?

JAMES: Yeah, I think it's getting in that area because it's not quite that blanket prohibition that ties everybody's hands. So I think we're getting closer.

JANIS KARKLINS: Okay.

JAMES: I want to talk with the other registrars.

JANIS KARKLINS: Yeah. I'm not pushing it. I'm just suggesting. Greg, is it something that you could look at it?

GREG AARON: Yeah, we can work on this. It might need a tweak. We may need a point[er] to the other building block, where we have the SLAs.

JANIS KARKLINS: Okay. Let's them maybe put this for the moment on hold and let it sink in. We may revisit it after the lunch break, simply to see what additional

tweaks we need to do. Then, if Greg and James could indicate what additional elements we need to add in which building block to Caitlin and Marika, that would be of great help already to put some placeholders in those building blocks.

We would revisit this sub-point, T, after the lunchbreak. I ask interested parties simply to consult among themselves on whether that is something they can live with.

Let me now go to U. We discussed that the fee structure we would put in the fee section, leaving here only one general principle, that the accreditation service be part of the cost recovery system. And "For further detail, see the financial stability building block."

Would that be something we can agree on? Here the most important part is the cost recovery, of course, not pointers to the other building block.

Okay. So then the principle is agreed to. Then the details we will be [looking] in the other building block [for].

Now we have V. This is the new formulation, that SSAD must have the technical capability of recognizing accredited requesters within the system. In addition, RDAP must facilitate the identification of accredited users. So that is in response to the charter question of the compatibility of SSAD and RDAP.

Marika?

MARIKA KONINGS: Thanks, Janis. While everyone is thinking about this one, again, some background. I think there was some back and forth and then there's quite a lengthy chat of comments on this issue. I think both Mark and I think Hadia worked on this. I believe last time around we put this in brackets because I think there was also a notion of, is this needed? I think we tried to insert something here to be responsive to a specific charter question that related to RDAP, but I think some people questioned whether the group actually needed to address that. So I think the question is, is this language needed here? Is it needed somewhere else? Or is it needed at all.

JANIS KARKLINS: My question, Marika. Can we not answer the charter question? I think we should.

MARIKA KONINGS: Well, I think the report would need to address why the group believes no specific response is needed because it's maybe already addressed through the implementation or RDAP because I know that's a parallel track that has taken place since the charter was developed. Of course, the group needs to answer the question, but the answer may be, "We have not answered it because we believe that it's already addressed through this," or the other.

JANIS KARKLINS: Okay, thanks. I have Hadia and Alex. I think that Stephanie's hand is an old one.

HADIA ELMINIAWI: Personally, I see that this item is not necessary at all because, if we are talking about a system like the one that was, for example, proposed to the European Data Protection Board, the unified access model or the standardized system for access and disclosure is built on the idea of having an accreditation system. So to say SSAD must have the technical capability of recognizing accredited requesters is redundant. But we can say it anyway if we need to respond to the question. But it doesn't really add anything.

Also, we could again say that RDAP must be able to identify accredited requesters, but again, this is obvious. But we can say it. There's no harm in saying it.

As part for the part I put in brackets, I think we don't need it now because, according to the system that was presented to the European Data Protection Board, actually the contracted parties will not be receiving the credentials. This was a question actually that we were trying to think of. Will the contracted parties receive the credentials if they don't need to receive them? So maybe this part we cannot really address now because we don't know yet the type of system or the kind of system that we're talking about.

So the first two lines are obvious, but if we just need to respond, let's put them in there. The others we cannot talk about yet because we don't know the system that we're talking about. Thank you.

JANIS KARKLINS: Thank you, Hadia. Alex?

ALEX DEACON: Thanks. Just on Point V, I think, Marika, what we could do – I think you alluded to this – is reference the TSG report, which suggests a mechanism on how RDAP could actually facilitate identification of accredited users and the like. That was the first step in answering this question. We could reference their report. We may also want to reference the work happening in the RDAP Profile Working Group, which actually now is just called the RDAP Working Group, that will be taking on some of this work or considering some of this work in the future and has identified a technical mechanism to enable RDAP to do all of this.

So I think there are options there. I would help you with this if you want. I think it's important we answer the question, but probably pointing to work that's already happened is the best way to do it.

JANIS KARKLINS: So then your suggestion and Hadia's would be not to put V and W here but then in the initial report simply to add a pointer to places where this work is done already? Could that be? If we would strike out V and W and, in the initial report, we would have a paragraph answering the charter question pointing where this issue is dealt with in our opinion. So then we will proceed accordingly.

I have Stephanie's old hand, Hadia's hand. Marc's hand is a new one.

MARC ANDERSON: Thanks, Janis. I think I like the approach you just described. I think that's more in line with what the charter is getting to. I think trying to answer that particular charter question here isn't a great fit. I think the charter question is getting at reminding the EPDP members not to build a system that RDAP can't support. I think your suggestion of taking it out here and making sure we account for it in a later section of the report makes sense. So I think that's a good approach.

JANIS KARKLINS: Thank you. So then we will do that. Staff took note. I understand that Alex will help in drafting the proposed part of the initial report, which will not be part of the building block.

Let us then move to implementation guidance in relation to accreditation. "The team provides the following implementation guidance." So, small A. Any issue with small A?

No comments? Hasn't been any comment also submitted in the Google Doc. So we're fine with A?

Marc Anderson?

MARC ANDERSON: Thanks, Janis. Matt and I were just talking about this one. I think what we're talking about in A would be referred to as identity providers in other sections. Do we want to just state that here for clarity?

JANIS KARKLINS: As Marika is now typing in, "authority as identity providers and/or verify information." Okay.

Sub-Point B.

Chris?

CHRIS LEWIS-EVANS: I think I'll just repeat what Marc said for the last one. I think it fits in this one as well because the accreditation authority won't want those details. It'll be the identity provider, I think.

JANIS KARKLINS: Thank you, Chris, for this remark. With the text now on the screen, would that be something we could live with?

Okay. Then let me move to C on auditing and logging. Any comments?

Volker?

VOLKER GREIMANN: Just the usual, that "organizations" should be replaced by "entities."

JANIS KARKLINS: You're so picky. Thank you for that. James?

JAMES: Thanks. I was going to raise my hand. Apologies if this is a first day of school question that I missed, but are we talking about two classes of accreditation, where an organization is accredited and then individuals from that organization use that accreditation? Or would they have their own accreditation as a parent-child relationship? I'm not really quite clear on how those work. Maybe this isn't the right point to bring it up. I'll just hold that question. But I'm still not really clear how those work. Thanks.

JANIS KARKLINS: Maybe that is something that we want to think of and maybe not define or maybe we want to define. Actually your question reminded me of another homework piece that has been given to the GAC: to help us with the accreditation of law enforcement, since this is something that we have not addressed, not yet. So if you could tell us where you are with your reflection.

CHRIS LEWIS-EVANS: Thanks, Janis. Just to respond very quickly. Our framework went to the GAC today and we will be discussing it tomorrow. Hopefully, off the back of that, we'll be able to provide something fairly shortly afterwards.

JANIS KARKLINS: So then on Monday we may except that we will have something. Good. I have a few requests on – now I'm not clear on the question of James o C. But let me take them. Farzaneh, Alex, and Milton.

FARZANEH BADII: Thank you. Sorry. As we are talking about C, I have a comment on D. Is that okay?

JANIS KARKLINS: We'll get to D. I will keep you in mind.

FARZANEH BADII: Okay. I will wait for mine.

JANIS KARKLINS: So we are now on C.

FARZANEH BADII: Okay. Thank you.

JANIS KARKLINS: If Alex or Milton – Milton does not have … Alex, you have, on C, a comment?

ALEX DEACON: I wanted to comment on James' first day of school question around legal persons or individuals.

JANIS KARKLINS: Maybe let's take C and D and E, and then we will come back to James' first day of school question. On C, it seems that we don't have … Let us move to D.

Ah, Thomas, we're using Zoom. I'm looking mostly to the Zoom.

THOMAS RICKERT: Yeah. I need to get back into the Zoom room. I was kicked out. I'm just wondering. "will be logged by the SSAD." Don't we need to specify that all parties that are involved in responding to the query need to do the logging? Because the SSAD is not defined so far. Is it a just a central unit? In my view, both the central unit, as well as the contracted parties that are involved in the disclosure request, need to log. Just talking about the SSAD doesn't clarify who is actually supposed to do the logging.

JANIS KARKLINS: So then, if we remove "by the SSAD," then we're leaving it broadly open. Then becomes an implementation question.

THOMAS RICKERT: Well, we could say "would be logged by all those involved in processing the query."

JANIS KARKLINS: Any issue with clarification instead of "by SSAD"?

Body language suggests no. Some say yes. Some say no. Chris, you say no?

CHRIS LEWINS-EVANS: Yeah. We're trying data minimization and everything else. You don't want every party involved in the SSAD query/logging query activity. That needs to be logged by responsible parties for that. An identity provider doesn't need to log query activity, for example. So saying "all" I think is wrong. I think we need to be more precise than that. Thank you.

JANIS KARKLINS: If we say that the query activity by all accredited entities would be logged as appropriate? And then leave it to implementation?

Greg?

GREG AARON: Logging is going to be an important part of this centralized system because it has to know what queries came in and when they got served and came back out. There's also a compliance function required. So at least this centralized system has to. That's probably important to say.

JANIS KARKLINS: This logging is specifically related to accreditation activities. We have a building block on logging of requests. With that understanding, I think we need also to – actually, I think we need to rethink all these distinctions. Let me pause a little bit here.

I will ask Marika maybe to clarify where this came from and why it is there – but I think that I have a competitor here who tries to talk at the same time when I do. Let's take Marika's comments.

MARIKA KONINGS: Thanks, Janis. The quick chat that we had here is that we had a bit of confusion over how this is worded because this is specifically to the accreditation block. So the question is, should this actually focus on auditing and logging by the accreditation authority, as well as the identity provider, in relation to how they managed the accreditation process? I think the way it's currently worded mixes the two things: the general logging and queries, which we're dealing with, and the separate building block of auditing and logging. I think here D and E are more focused on the aspect of the accreditation process.

So maybe we should take this offline, or, if people have initial insights on whether, as part of the accreditation block, we should also spell out what kind of auditing or logging requirements apply to do the accreditation authority and the identity provider and whether that needs to be included here. And try to avoid mixing the two things.

JANIS KARKLINS: I have four hands up. Farzaneh, Alex, Deacon, Alex, Alan Woods, and Georgios. I will take them in that order. Farzaneh?

Oh, sorry. Okay. Alex?

ALEX DEACON: I've been thinking about the question or the comment that James made. I note that B says, "Accredited entities may be legal persons or individuals," and I think there's some unpacking we probably need to do there. My assumption is that this means that a credential to access the SSAD could be issued to an individual, like Alex Deacon, or to a legal entity, like Cole Valley Consulting, or some other large organization. That single credential would be used to access the system. So there's probably some more thinking that we need to do there and maybe some more specificity with regard to the policy of what that actually means.

JANIS KARKLINS: Let me make a suggestion. Let us forget for the moment about C, D, an E but address conceptually the question of James and what Alex just commented on. Accreditation … For instance, if there is a small or medium-sized organization versus a big organization with many units that may be requesting the personal data, how could that be organized in different sized organizations? So just a free-flowing conversation, conceptual. Hands down, those who have them up. On this free-flow conversation, hands up again.

Alan and Matthew. Alan?

ALAN WOODS: Sorry. I'm not clear. What I'm supposed to [comment on]? Apologies.

JANIS KARKLINS: About James' question on how [inaudible].

ALAN WOODS: Oh, no. Hands down on that one.

JANIS KARKLINS: So hands down. James?

JAMES: I'll put my hand up and rescue my friend Alan. Maybe I don't want to make this overly complicated if it doesn't need to be. If it's a simple case of that either a natural person or a legal person can be an accredited user of the system and, if you work for an organization and you know the credentials and you can use them, then you are representing that organization in your use of the system and you are attaching liability for the use of the data is disclosed to that organization and you're essentially acting on behalf of that organization. We can say that, and we can say that this is fine and move on.

I just wasn't clear when we had it on a previous bullet point. It sounded as though there were ways or situations or scenarios where we would de-accredit an organization but there would still be accredited individuals at that organization. That's where I started to get a little confused. I thought, "Is there an organizational container which is holding individual credentials? Or, are they separate and distinct and, for example, I could have my own accreditation and then some

organization that I was associated with would have its own accreditation as well?"

If we want to just say that that's the simplest approach, that's fine. Then I think that takes us out of a lot of different thorny questions about what to do when they're de-accredited.

So that's just one thought. The concern would be, is that open to abuse? For example, if I had an organization with 500 employees, would it make sense for me to get one accreditation for the organization or 500 individual accreditations of the employees? I just opens up some other interesting things. But we can leave it alone. It was something that I was just not understand completely.

JANIS KARKLINS: We can imagine that that would be an internal organizational policy issue. So, if an organization considers filing five accreditations, for instance, and then lets a subset of staff use one and a subset of staff use another, that would be their internal thing.

We may also think in terms of law enforcement. They may consider giving one organization as a contact point. Then that would be a gateway for law enforcement of that country to file through that gate, and we would not know who is behind it. We would know only that that specific liaison is the one that filed the request and so on.

Again, there may be a multiplicity of options. The question is, can we, let's say, identify all possibilities to describe in the policy? Or do we

leave simply at the discretion of each organization/entity to decide what type of accreditation they would develop themselves?

[JAMES]: Janis, could I respond very quick, please?

JANIS KARKLINS: Yes.

[JAMES]: That works perfectly fine. The only caveat would be as long as it's clear that individuals using an organization's credentials are doing so on behalf of the organization because I can see where sanctions would come own and they would say, "Well, it wasn't us. It was this employee. They're fired now, so all good, right?" No, not all good. They were acting on your behalf.

JANIS KARKLINS: Okay. Alex and Hadia?

ALEX DEACON: I definitely agree with James that we should keep it simple. If adding the language that you just suggested helps – I think it does – then we should do that.

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

HADIA ELMINIAWI: I never actually understood it the way James is explaining it. If there is actually a possibility that it could be understood in that way, then it should be clarified. I don't know actually which text made you explain it in that way. But, if it exists, then, yes, we should modify it. Thank you.

JANIS KARKLINS: Based on this conversation, I think staff will propose one sentence in one of the points. Maybe it's in C. Or wherever it belongs. We will show that sentence for our approval at the time when we will be talking about T, not tea as a drink but T as a point in the text.

We have come to the time when we want to get the lunch boxes. Here priority is to the team members. So we have a lunch break now.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: Sorry?

UNIDENTIFIED FEMALE: [inaudible] lunch.

JANIS KARKLINS: Yeah. We have a lunch break now, but as usual, there is no free lunch. We will be working, though we will give a 15-minute bio break. I would

suggest that we grab the lunch boxes that were brought here. As I said, priority is with the team members.

After 15 minutes, those who are interested in a conversation with ICANN org on terms of reference for legal/natural study, please come back. For those who are not very interested, please eat your lunch boxes wherever you want. Then we will spend about 30 minutes listening and providing input/first impressions on the terms of reference.

For the moment, it is the lunch break. We restart in 15 minutes with the conversation with ICANN org on the terms of reference. Thank you.

Okay, guys. We will engage now in the conversation with ICANN org, represented by Karen Lentz. We will listen to maybe the initial thoughts on ICANN org on the draft terms of reference for the study that has been commissioned by the first phase on legal versus natural persons. After this presentation, those who will have any initial reactions will be able to provide in the formulation of those terms of reference.

Also, Karen, if you have some idea on the timeline of the study – I don't know whether that is part of your presentation – if you could also address that issue as well. Thank you. The floor is yours.

KAREN LENTZ: Thank you, Janis. I'm here to talk about the study plans in reference to – is this echoing? – Recommendation 7.2 from Phase 1. We'll recap the background of Recommendation 17, go through the draft terms of reference that we've developed and then have a discussion and questions from the team.

As background, this was in relation to the one of the Phase 1 charter questions concerning if contracted parties be allowed or required to treat legal and natural persons differently and what mechanism is needed to ensure reliable determination of status.

We reviewed not only the recommendation but the discussion in the Phase 1 final report on the team's deliberations on this topic and noted that there was a question submitted to legal counsel self-identification by the registrant and potential liability there. The response was that parties could be subject to liability if the regis[trant] were to wrongly self-identify and provided some potential suggestions for how that could be mitigated, such as a mechanism for correcting information using technical tools, etc.

The policy recommendation in 17, in response to this charter question, had three parts. One was that contracted parties, registries, and registrars would be permitted to differentiate between registrations of legal and natural persons but not obligated to do so. So that's the recommendation that's being implemented as part of Phase 1.

17.2 suggests that ICANN org carry out a study on the cost and benefits of differentiating with the terms of reference to be developed in consultation with the community and to consider the following: feasibility and costs, including implementation and potential liability costs of differentiating between legal and natural persons, examples of industries or other organizations that successfully differentiated, privacy risks to registered name holders of differentiating between

legal and natural persons, and other potential risks to registries and registrars of not differentiating.

Finally, Part 3 notes that the team will determine/resolve the legal versus natural issue in Phase 2.

So that is the background of the recommendation. What I'm sharing in terms of the draft terms of reference is our interpretation of what was being requested in the recommendation to help inform the Phase 2 team's work. [inaudible] is that this is a draft based on our interpretation and that comments and input from this team are certainly encouraged.

The objective here for the terms of reference is to complete a study that informs all of your deliberations on potential policy recommendations regarding differentiating between legal and natural persons in the handling of registration data.

The scope includes the things that were listed in the recommendation. That would include identification, feasibility considerations related to the differentiation between legal and natural persons in registration data systems, identification of potential legal liabilities associated with differentiating one or more case studies of organizations that have differentiated and any insights generated by this experience, and an examination of the potential risks and scenarios with and without differentiation.

The goal of this report is to be an input to the EPDP team's Phase 2 work on this issue. I'll emphasize the last sentence on there, which says that

providing recommendations or normative assessments as to the differentiation of legal/persons is not in scope for the study. So the study is meant to be informational as an input to this team.

Working definitions. These are the working definitions that we've adopted for the purposes of the terms of references. A natural person versus a legal person. We actually didn't find a definition in the report or in the GDPR, so the definition that you see here is taken from a legal journal that discussed these terms. But if there is a reference that we should be using in terms of definitions, that would be helpful.

Research questions. This is how we have proposed setting up the study. The recommendation poses two scenarios, one being that registries and registrars may differentiate. This is the current recommendation, 17.1. The second scenario is a scenario where registries and registrars are required to differentiate between legal and natural persons.

Based on the recommendations, the questions are termed according to these three components that were part of the recommendations, looking at feasibility, costs, and risks. To break down how we would look at these things are some additional detail. So, in terms of figuring out what the feasibility is of these different scenarios, that includes both looking at operations and looking at implementation. So, for each of the scenarios, what kind of systems or procedures or standards would be required and how would they differ according to the two scenarios and how does the operating environment – for example, gTLD or ccTLD – and the jurisdiction affect the feasibility component.

Also, considering in each scenario what kind of communication or education would be needed to make that system work to ensure that registrants understand how their data is being processed and what choices they're making as part of that system.

In looking at costs, we've broken that down in terms of monetary and human resource costs, as well as cost allocation. So, for each scenario, what would be the cost of implementing something new? What would be needed to continue operating a system under these scenarios? And, again, how would the operating environment or jurisdiction affect those costs for cost allocation, considering not only what the costs are but how they get distributed among the different parts of the system.

Risks we've looked at as suggested in the recommendation – the privacy risk. So what legal liability and other risks are there relating to registrant privacy? How are those affected by the operating environment and jurisdiction? Looking also at what would be the impact of errors, what would be the components that could lend themselves or would be affected by criminal activity, how would that play out in the system and, again, how do the operating environment and jurisdiction affect those risks.

This is the schema that we have come up with, which is something that we would look at in both of the scenarios according to feasibility, costs, and risks. The top part is the stakeholders that we've identified. So it's not only if you ask a question about cost or feasible. The question is, feasible for whom? Or cost to whom? So we've proposed here looking at these things in terms of the registries and registrars and how are they

impacted and how are the data subjected impacts and how would end users of data be impacted in these different scenarios. This schema is to guide all of the questions that would need to be asked, not necessarily to just fill in a table. But this is how the structure would cover all of these things in the two scenarios.

We've compiled some potential information sources. A few of those are several of those listed here. I'll go through those quickly. Literature review of current reports or sources that are relevant – who has thought about this before, written about this before. Requested information that we could directly request from registrars – cc/gTLD registrar operators – asking what changes have been made, what changes would need to be made, in the event of a change to policy on treatment of legal and natural persons. That could include direct, in-depth interviews, both with entities who do or don't currently differentiate. That could include outreach to users of registration data, inputs from data protection authorities – you've already had some of those – some type of survey, review of current and pending legislation, and a survey looking at other industries or organizations that process personal data and do distinguish between legal and natural persons.

In terms of the deliverables, this is how we've conceived that the report would look. It would include, first of all, a baseline description of the registration system – how it works, who are the parties involved, methodology, describing how the analysis was undertaken in the study. The third part would be the substantive look at the questions that were described. So, under these different policy scenarios, what would the impact be? This is a model-based approach, so, if you look at all of these

questions as part of a system, if you change a variable at the policy level, what are the impacts throughout the system?

Finally, I wanted to mention a few constraints in looking at how we might carry out this study. One is in the area of quantitative analysis. We think, to the extent that we're trying to get numbers focused on the monetary costs of different scenarios, this may be difficult to get, as they concern proprietary processes. So there may not be a lot of information that we have to work with in terms of numerical assessment of costs, also noting that looking at the liability costs of differentiating will vary among the global jurisdictions. So, presuming that it's not practical to look at every jurisdictional and how this type of liability might be assessed, there is potential to, for example, do a couple of case studies looking at those questions in detail. Then we've noted that, in performing a study, we should seek to mitigate these limitations and know where there's not sufficient data to provide a comprehensive analysis. So, noting what's missing.

That brings us to questions and discussion. I will raise a few questions here. One of them has to do with process. Janis asked about the timeline. In terms of process, the recommendation asked for the terms of reference to be developed in consultation with the community. As this team is the intended audience for this study, I think this is the primary group of interest in terms of helping develop the terms of reference. So, wanting to understand that piece of the process, as well as, for example, if we do the study, is it expected to go through public comment before being provided to this team as a deliverable.

In terms of a timeline, we really don't have one at this point because we're seeking to understand here what's really required by the team and that the timing will vary.

One of the other questions that we had to raise here was, what kind of qualifications are sought after in terms of performing the study? I've heard discussions of ICANN org doing a survey versus performing a risk analysis. There's some legal liability questions which might be a different set of expertise or a different set of needs. So is there potential to having this study done in pieces, or is it expected that we engage someone to perform all of these things?

So these are a few of the questions that we have. With that, I will turn it back over to the Chair for any questions and discussion. Thank you.

JANIS KARKLINS: Thank you, Karen. Now the floor is open.

Matthew?

MATTHEW: Thanks. I appreciate you sharing this. I think it's super helpful. I just had one question. The first slide, I think, talked about a piece of this being assessing the privacy risk and potential legal issues or legal liability. But then on the sources of information slide, I didn't see any reference to working with outside counsel or any sort of legal sources.

So I'm just curious. Is the plan to either rely on the advice that we already have on this issue? Is the expectation that we may go get

additional legal advice on this issue? Or is that a question that ICANN org is going to handle internally? Thanks.

KAREN LENTZ: Thank you. That actually goes to a question that we had in terms of a study to help assess the liability risks because we did note that there was been at least one legal opinion provided addressing this. So is the goal to collect many legal opinions or to try to reach some sort of consensus among the legal opinions on this question? That's the question that we were looking for guidance from the team on.

JANIS KARKLINS: Thank you. Alan Greenberg, Milton, Greg, and then Brian, Margie, and Laureen.

ALAN GREENBERG: Thank you. Karen, I appreciate the difficulty of giving us a timeline, given the unknowns you have. Can you give us a range of optimal versus long? My experience with ICANN and the studies is that the good ones can take six months. The long ones can take two to three years. I've seen studies done for ATRT which have a one-year finite time, where their study gets done in a few months. It's rather rushed and it doesn't … I'm not convinced we're going to make one of those really short timelines, but can you give us a range? Because, if we can't do our work until we get this study back, how long are we being asked to be participants in this [C-PDP]? Just give us some idea of timelines based on your experience.

KAREN LENTZ: Thank you, Alan. I think, to the extent that we have started to gather some of the information from the pieces that we've listed here and that our assessment of the timeline is, again, based on then qualifications and whether we're planning to go out and find one or more entities to do this, which is separate from the time that it would take to actually do the study, to do the study, starting from Day 1 with the resources in place, the range from the simple end to the more complicated end would probably be three months at the lower end and nine months at the higher end. That's my estimate at this point.

JANIS KARKLINS: Okay. Let's hope that that would be in the lower end. Michael? Milton? Milton, please.

MILTON MUELLER: As somebody who does research and design studies, I wonder if you mind if I go down this list of potential information sources and ask you what you had in mind in each case. I would begin with the question of, which one of these information sources is actually going to give you data about the potential risk to data subjects of differentiating between legal and natural?

KAREN LENTZ: I think that's somewhat of a hard insight to get at. I think, if you have other sources to suggest, that would be great. But in terms of what we

envision, I think part of that comes from the legal analysis, looking at it from a legal perspective: what are the risks? I think other writings or research or interviews may yield some of that, but I think, again, if you have ideas to supplement that, that would be great.

MILTON MUELLER: Okay. Excuse me if you've already answer this, but it wasn't clear to me – you've done quite a pretty good job of defining a methodology and data sources for this study. Were you thinking of outsourcing this or doing this internally?

KAREN LENTZ: That's actually one of the questions that we had in terms of if there were certain expectations as far as qualifications, be they in the law or in risk analysis or other areas. So, if the goal is to perform a survey, I think that's something that probably ICANN org could readily support. If there's specific types of expertise are thought that we might not have, then I think we would be looking for someone else to supplement that.

MILTON MUELLER: Okay. What does "survey for lessons and examples" mean in this case?

KAREN LENTZ: Surveys were mentioned a few times as ways that we could go about doing this. I think it's actually repetitive of the second and third bullet. So, if we're looking at entities who are already differentiating or not

differentiating, it's to take a survey around what they may have learned or examples of issues that they may have had in that.

MILTON MUELLER: I notice that the only people you're not surveying are the data subjects themselves. Is that correct?

KAREN LENTZ: Well, I think it's not intentional. I think that, if there's a way – I'm taking data subjects here in this discussion as meaning the registrant who's providing their registration data. I think they're definitely a part of the stakeholders that should be considered in the schema slide. In that one, the data subjects are considered there.

MILTON MUELLER: Yeah, that was good. I liked that. That's a good schema. I like it. Okay, that's all. Thanks.

JANIS KARKLINS: Thank you. Greg is next.

GREG AARON: First, Karen, thank you for the presentation. One of the starting points is that Phase 1 memo from Byrd & Byrd about natural versus legal. One of the things it did was it said there are probably a range of options that might satisfy the law, ranging from some sort of a minimum to a

maximum. So we need those broken out see what the spread of options is because those involve different tasks.

When looking at costs, there are a couple of different ways to define that. One is a cost in terms of "Here's a task that needs to be done" and you could also try to associate maybe a dollar amount or euros with fulfilling that task. Probably listing the tasks is easily and relatively non-controversial, like a registrar is going to have to ask its registrants what category they fall into and give them a mechanism to change or update their self-identification. That kind of thing. Assigning dollar amounts is going to be controversial. That's all I'll say about that. So certainly laying out the tasks is something we could probably all agree with.

One of the sources that you should look at and talk to are the RIRs. SSAC can give you the references for their policies because they have policies that allow the data of natural persons to appear in their contact records, which are published publicly. So we'll send you the references to their legal policies.

It'd probably be a good idea, if possible, to have Byrd & Byrd involved because part of this activity is about risk evaluation and they should at least vet what we're doing as we go along. Then, at some point, we want to see a draft of it and then provide input. Thank you.

JANIS KARKLINS: Thank you, Greg. So you have a lot of help coming from SSAC. Let me take Brian next.

BRIAN: Thanks, Janis. Thank you for presenting this to us. I think this is really good. I would add a couple suggestions. I love to agree with Milton every time I can, so I think it is important, especially in re-reading the Byrd & Byrd memo. The whole thing seems to turn on how much information the registrant has when they're providing that and whether there's any doubt as to whether they understand the consequences of that. So there's some good language in the Byrd & Byrd memo about how to look at that through the registrant perspective. I think that's important.

One suggestion I have in addition to that is I think it would be helpful if this study assumed that the privacy proxy services accreditation was implemented. I think that really could be helpful if the privacy proxy data, because it's in the WHOIS record for such a large number of domain name registrations, provider was accredited and known and that WHOIS information could be tied to that privacy proxy provide. That won't be personal data. That'll be legal person data. That's such a large percentage of the gTLD domain base that I think that'll be helpful in informing the study.

Just as a note for the group, I think that it sounds to me, I think because this is coming from the Phase 1 policy, that this is research vis-à-vis the potential for contracted parties to make the legal/natural distinction. I think we should think about in this group whether it makes sense to use this analysis when it's finished and then think about whether SSAD could also make this distinction between legal and natural persons. Thanks.

JANIS KARKLINS: Thanks, Brian. Laureen is next.

LAUREEN KAPIN: Thanks. I also want to reiterate the thank yous. I know a lot of thought and effort goes into thinking about this and being very specific.

I wanted to echo the recommendation about using legal counsel for certain parts of this, particularly the surveys of legislation and the assessment of risks. That seems to me to be a legal function and the folks who could do that most efficiently.

The other issue I wanted to raise is in terms of the impacted entities. We have contracted parties, data subjects, of course, data end users, but I also wanted to reflect that the public at large has an interest here. Just as data users have an interest in privacy, the public at large has an interest in access to this information. If large portions of information that arguably aren't required to be shielded are shielded, that does have an impact on the public. That isn't present here or being visibly considered, so I wanted to raise that. I realize it may be hard to measure, but I think it's very important to keep that in mind. That really is the other side of the coin when we're talking about the public interest. The public has an interest in privacy, of course. The public also has an interest in the human right of security and not being a victim of crime and deception. So I wanted to make sure that that is surfaced rather than just in the penumbra here. Thanks.

JANIS KARKLINS: Thank you, Laureen. Let me take the next one: Thomas followed by Alan Greenberg.

THOMAS RICKERT: Thanks very much. Great work. This is very interesting. I'm afraid that you're embarking on a massive undertaking with this. I'm wondering whether that's something that we should actually task you to do for two reasons. I think that mitigating risk for new registration data is pretty possible. I could think of various ways of properly informing the users, making them aware of the distinction. They should tick some boxes and what have you. That would potentially change the registration process slightly. But I think that risk can be controlled. A lot of cc's are doing it today.

The big risk that we have – I don't think that you've made this distinction here – is how do we deal with legacy data? For that, I think we would likely not get a clear answer because there will be scenarios in which we will fail. Or, even if we don't, there might be registrants who think that they are inappropriately dealt with that still might raise claims, justified or not. But you might have some efforts in defending against those claims.

So my question is, do we want to even split this study to deal with data to be collected in the future versus the legacy data and how to deal with that? If we did so, how are we going to deal with the results? Because we would likely get an output of the study that will not make everybody happy around this table. As we've seen with the legal advice that we got, we get the legal advice hoping that we can make a third party make

a decision for us and still we're not going to accept it. So is this going to help us in any way if we can predict that our group or parts of group would likely not accept for a fact the outcome of that and live by it.

JANIS KARKLINS: Thank you, Thomas, for this open-ended question.

THOMAS RICKERT: I can make it less open-ended. I would maybe take this back before we start the big thing costing ICANN org a lot of resources, costing a lot of external resources that we need to budget for. Let's try to boil this down to what we absolutely need and then do a roll call if we're going to accept whatever the outcome of the study is going to be because, if we're not making a commitment as to using that as a basis for our policy making, then we're none the wiser. Then it's just ink on paper.

JANIS KARKLINS: Thank you for this wise advice. Alan Greenberg?

ALAN GREENBERG: Thank you. The more I listen here, the more trepidation I have at a number of levels. I don't think we can avoid doing it. I think it's a crucial question that we have to ask. When Alan Woods gave us a description of how we handles queries, the vast majority of them ended up being, "Oh, GDPR is not applicable. I can release the data." Therefore, we are clearly redacting a lot more than we need to, based on the law. So I don't think we can avoid doing it, no matter how messy it is.

I put my hand up again, though, to add something to the timeline. You said three to six months once we start the actual work. Just for those who do not know, if we have to go outside – I'm thinking that, for at least part of this, we will have to go outside – ICANN has rather lengthy procedures associated with selecting vendors and signing contracts with them. So I think we're going to have to talk amongst ourselves about how we're going to deal with this study, which I believe is essential. But we probably will not get any results back for six months, optimally, and perhaps another six months after that. Thank you.

JANIS KARKLINS: Thank you, Alan. Farzaneh?

FARZANEH BADII: Thank you. I agree with Thomas' point, with all of them. Also, I want us to be clear about the purpose on what we want to do with this study. What is the point of differentiation? So we don't not redact the organizations, and the end users can have access to it easily? It is the point to have access to this data more easily? So that's the point? Are we not working on an access system so that you can easily have access to data regardless of this differentiation? I have raised this point multiple times. Not getting anywhere.

Now, if I comment on the study itself, I really like chart. However, I think that there are problems with surveying and asking the data subjects what is their understanding of the privacy implications because most of the time when the data subject is not actually in the process of

registering the domain name [and] has another perception and thinks "Yeah, sure. I know [the] time and organization" … But when they are actually in the process or registering a domain name, they might know or not consent in an informed manner. So just asking them direct questions I don't think is going to get you anywhere about the implications that it might have for their privacy.

What I would suggest is to look at how the operation of the different registries and registrars work when they do differentiate and survey the data subjects that did it wrong or had complaints about it.

The other point that I think is very important is to clear your methodology because, as you talk about surveys and also those information sources you had on your other slide, if you could, based on this chart, also differentiate the sources that you're going to have a look at – for example, for data subjects, what you're going to look at [is] if they're the same as the other contracted party and data and users or if they are different [inaudible] … Thank you.

JANIS KARKLINS: Thank you, Farzaneh. Stephanie?

STEPHANIE PERRIN: Thanks very much. Thomas had made some of my points. The problem with the huge amount of bad legacy data – I say "bad" meaning A) it's inaccurate (we know it's inaccurate) and B) the individuals who are not necessarily informed … Remember, we're trying to inform a global population about the GDPR, which they are not likely to understand.

I'm not even sure we could all in this room pass GDPR quiz at this point in time. Certainly our registrants couldn't. So that' a problem. I think you need to separate that out.

The other thing that concerns me is that this bad legacy data is going to taint a lot of your other qualitative information. If you go out and talk to people about their experiences, A) could they pass the GDPR quiz and B) did the experiment that they tried in differentiating comply with based on bad legacy data and did it comply with GDRP? So a lot of your qualitative data is going to be compromised.

By the way, first of all, thank you for doing all this work and laying this out. I don't often agree with Alan, so let the drum roll come now. Alan Greenberg, I agree. Sooner or later, we have to do this work. But the idea that we're going to get a decent study done in time to enlighten our efforts here I think may be flawed.

The other distinction I wanted to make is, really, let's try to narrow this down to the difficult chunk. Proctor & Gamble knows they're a company, right? So the big brands can we put in one bucket? I keep saying – I'll say it one more time – big brands can authenticate themselves with their corporation numbers, their business numbers, their whatever. They can do that. Easy. "Get those guys covered and put all the data out there." I'm not so sure about the domainers that are complaining that they can't put their For Sale sign out. That's a different problem, depending on how they set up their tax status.

That brings me to my third point that you really need to look at the wide [ambit] of what's going on here. You have to make a very clear

distinction between what a website is doing and what a registration is doing. A lot of the consumer complaints are based on a website that may or may not be linked to the individual that has the domain name registered. That may be deliberate because they're crooks or it may be accidental. It could be anything. So that has to be a [bright] line, and I don't see that in the methodology. So I just want to nag about that one more time.

I think that, realistically, are there pieces of this that would enlighten our work at the moment. There was a study done way back in the PPSAI days. I complained about it vociferously because it wasn't, in my view, a good study and it was an ambush that came at the last minute and was included in the record.

But just knowing how a large number/assortment of jurisdictions make the distinction between what they call a legal person and what they call a natural person and whether they have any data protection law and whether in fact they also cover employees of companies in the same way as if they were natural persons might be useful. That is doable study that we could have within a reasonable timeframe, I think. That should be done by a law firm. Thanks.

JANIS KARKLINS: Thank you. Marc Anderson, followed by Margie.

MARC ANDERSON: Thanks, Janis. Just to echo what everyone else said, thanks for coming and presenting this to us. At first glance, first run through, this is excellent. You've obviously put a lot of thought into that.

On the slides, could you scroll to the last slide for a second? Sorry, the one before that. Yeah. I was wondering if you could expand a little bit on what you meant by the model-based analysis? I thought that was very interesting. So I was wondering if you could into that in a little more detail for us.

Then, if I could, a second question. Like I said, obviously you've given this a lot of thought and you're coming to us looking for some feedback, some guidance. I guess I'm wondering how we draw a bow on this. What are exactly the things that you see as inputs requested from us in order for you to move forward? Maybe you don't need to have answer that now. That might be better as a follow-up e-mail or if it's something you've given some thought to. I think that would be helpful in moving this forward.

KAREN LENTZ: Thank you, Marc. In terms of the model-based analysis, this is really based on the couple of scenarios that we're talking about with the different stakeholders and parts of the registration system that have been described elsewhere. For example, the model of "it's optional to differentiate" works a certain way, where you have a data subject performing a certain step and you have the registration service provider performing a certain step and so forth. So it's constructing that model and then looking at, if you change one of the pieces in the model, what

are the effect on the other parts of it. So it's really to identify what the impacts would be in terms of a model rather than trying to suggest something is feasible or not feasible or too risky or not risk enough or whatever.

In terms of the second question – what type of guidance? – I certainly understand the inputs around how long it will be until we have some inputs as a result of this study I think one of the things that would be great to get is what are the key questions? We talked about a lot of thing. Are there certain areas that are higher priority or are must-haves? Along the same lines, in terms of your timeline, is there a certain timeline that you suggest would be optimal in terms of planning your work? And what would that look like?

I hope that helps. Thanks.

JANIS KARKLINS: Thank you, Karen. We're headings towards the end of the session. I have two further interventions, Margie and Alan Woods.

MARGIE MILAM: I think this is great, but I think that, because of the timeline and what we've heard about wanting to get input quicker, I'd encourage you to take a lighter approach to this. I think that these questions probably should have been asked to us a long time ago. We filed our final report in February, I believe. The Board approved the recommendation in May. We're now five months later and this is the first we're getting these questions.

One of the reasons I bring this up is because I really think that, as we work on our policy recommendations going forward, ICANN org needs to be really active, talking to us and understanding our recommendations, so that, with the rest of our recommendations, we don't get to a place where, five months after they're adopted, we get these fundamental questions that haven't been answered. So let's just keep that in mind. As you guys are here at the table, raise your questions earlier because I do think that the legal and natural person distinction is important. We have it in our Phase 2 work.

One of the things to answer Farzaneh's is that, if we get to a place where we're comfortable with the risk we would have, it's the possibility of having either legal persons that are no longer being redacted across the board or, perhaps, when you do the 61F analysis, they get automated processing when a request is made. So it's actually very relevant to our work, so I do encourage you to do it and to do it quickly, sooner rather than later. That might mean a lighter-weight approach on the study because I know that ICANN studies can be very large and time-consuming and expensive, and I don't think that's what we were asking for in this case. Thank you.

JANIS KARKLINS: Thank you. [You're having an] applause, but from the different room. We have Alan Woods last.

ALAN WOODS: Thank you. I just wanted to very quickly actually redirect back to what Alan said earlier about the examples of me not having to do that. From a baseline point of view, I think it's clear that anybody in the CPH would be quite happy to have a system where that was possible and differentiable in that sense. I don't think your point was well-made out in the sense that it's not indicative of this problem. If we had the feasibility, if we had a way of saying, "Yeah, we can do this," then I think we would be very happy to implement that if we had that [covered]. So, for that reason, I really do welcome the excellent work that seems to have gone to this already, and I look forward to seeing where that comes from.

I suppose the other thing is I like to bring it back to asking that simple question of, "Well, what was the original point of the EPDP all those 17 millennia ago?" That was, of course, to take the temp spec and confirm based on what we had at the moment, [which wouldn't] bring it up to that level of "It applies with the GDPR." That was the major issue, and that did not necessarily envisage rewriting the system to allow for this. I think now we have a bit more time and we have a bit more luxury with the advent of this particular study that that could be focused into something that could create a situation where we can think more thoughtfully as to the differentiation and the delineation, not only the GDPR but in all other data protection. I'm seeing them jumping up all over the place. I saw India has one that's very similar, I believe, to the GDPR. All these things are coming through.

So, again, I think there's a mammoth task (that's to echo what a few people said) ahead of them in this one. I for one am really looking

forward to it. Therefore, I would like to see an in-depth study because I think it's a very good opportunity for us to consider this. Policy development will continue on, and our industry will continue to develop in line with this. I just don't want us to waste the opportunity of cutting off potentially a very valuable study that will help us all in the long run in terms of fitting into this small box of the EPDP itself.

Again, thank you so much. I look forward to seeing what comes from it.

JANIS KARKLINS: Thank you, Alan. In the meantime, Alan Greenberg has raised his hand. But, Alan, if you can do it very quickly.

ALAN GREENEBERG: I just wanted to raise one thing that I don't think we've talked about today but we've certainly talked a lot about in the EPDP, and that's that there's a concern that it may be clear that this is a legal entity, a legal person, that has done the registration but there may be personal information displayed in their contact address. There are some parties and some opinions that, if you as a legal person put personal data in, you are taking the risk and you are certifying that you indeed have permission to do it. There are other people, other opinions, that the registrar/registry would bear the risk because the information resides in their system.

Getting a better answer on that might help with making the decision a lot easier because then it just amounts to determining is this a legal person and not having to worry about what contents of the data might

be surrounding it. Thank you. So that may be something you want to consider as a fast path to helping us make the decision.

JANIS KARKLINS: Thank you very much, all who have spoken. I'm not sure whether it is in our mandate to overrule the decision of the council and the Board of not doing the study, because it has been decided to [be done] based on the recommendations of Phase 1.

I hope, Karen, this conversation was helpful to you. I don't know whether you want to say something in conclusion.

KAREN LENTZ: Yes. Thank you, Janis, and thank you, all, for your discussion and input. I think for a next step what I would propose is I will circulate an update terms of reference, taking into account some of the suggestions, particularly around specifically breaking out data sources and methodology for the different pieces that are described in there. Then we'll also, looking at the key questions that were mentioned, propose a sequence of events with a timeline that we can share with all of you.

So I appreciate the discussions. I have one other comment, not abut Recommendation 17, if I may, while I'm here. One of the other asks from Phase 1 of ICANN org was in relation to data retention. It's Recommendation 15.1. Org was asked to identity instances where we were asking for data beyond the life of the registration. That analysis we have completed and it should be circulated to this team shortly. So you can except that. Thank you.

JANIS KARKLINS: Thank you very much. I would say this made our lunch [worth it], right? So thank you very much, Karen. That concludes our lunchtime break. We will resume our working session in seven minutes from now. So a quarter past. Everyone who has raised hands now can lower them, please. There are still five hands up.

Team members, back to work. Team members, back to work. Technical team, we can start recording. My apologies for interrupting these lively discussions around the room. Now let's concentrate on the accreditation building block.

We have a few elements that we need to define. Then hopefully we will be able to say that the building block is stabilized. If I may ask to take off my picture from the screen and put the text on. We had this conversation about James' first school day question. The staff is suggesting the following formulation as is now seen on the screen. In B, accredited entities may be legal persons or individuals, and individuals accessing SSAD using the credentials of a legal person warrants that the individual is acting in the interest of said legal person.

Is that, James, what was your concern?

JAMES: Yes. Thank you, and thanks to Marika for, in between, hashing it out. I think that we could choose between "acting in the interest of said legal person" or "asking on behalf of legal person." I would defer to the many lawyers around the table if those are equivalent statements. I think the

key here is that the individual that uses the system with the organizational credentials is binding that organization to the consequences of the use and the terms of use. I just want to make sure that we've got that covered. If you feel good about "in the interest of" versus "on behalf of" … I don't think Volker feels good. He's shaking his head at me. Sorry. But that would be my only concern: that little phrase there. But otherwise I think it's great. Thank you, Marika.

JANIS KARKLINS: Thank you. Volker?

VOLKER GREIMANN: Just maybe two short words on the differentiation between the two. You can act in the interest of a third party without that third party ever knowing, but you cannot do that "on behalf of" [as] this very much stronger with relation to the third party as opposed to "in the interest of."

JANIS KARKLINS: So then we are putting "on behalf of." If that would gather consensus around the table on this specific point, then that would be our determination.

Yes? No?

UNIDENTIFIED FEMALE: [inaudible]

ALAN WOODS: Can I suggest, instead "on behalf of," "with the authority of said legal person"? Because that seems a bit more … Also, can we not use "said"? I know I'm a lawyer and we all love the word "said" – we can work on that obviously in the off times – but "said" this and "said" that? No. Plain English all the way.

UNIDENTIFIED MALE: For the record, it was a non-lawyer that put that in there. Sorry.

JANIS KARKLINS: What is then your suggestion? Alan? "acting on the authority of"?

ALAN WOODS: Yes. "acting on the authority of a legal person." I don't think we need to say "said." It's implied. Or "of the legal person."

UNIDENTIFIED MALE: "of the accredited legal person"?

ALAN WOODS: "of the accredited legal person." Yeah.

JANIS KARKLINS: Okay. Brian?

BRIAN: Thanks, Janis. It should probably be "the accredited entity," because the accredited entity might not be a legal person, either. So it should be "accredited entity."

JANIS KARKLINS: We're using "entity" throughout the text, so then let it be. Good. With a collective efforts of lawyers and non-lawyers around the table, we have formulated in addition and improved the text. May I take that this is our collective wish?

Yes. Thank you. So let us move then down the text. We have Q, I think. Alan?

ALAN GREENBERG: Just noticed there's another "legal person" just above it, halfway through the sentence.

JANIS KARKLINS: Okay. Thank you.

MATTHEW CROSSMAN: I think we've actually created a bit of an issue here that I think we may be able to clean up just with a little find-and-replace. But in other places in the document we've changed. We've used "entity" to distinguish between an individual credential and an entity credential, whereas here we're talking about accredited entities, including both legal persons and individuals. So I think maybe we just need to make a

decision. If we use “accredited entities” here as that umbrella term, then maybe we do go back and change “entity” where it’s used elsewhere to “organization,” for example, just so that we’re not creating confusion. Does that make sense?

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: I think that this is something that we can rely on staff for, asking staff to go through and clean up without the changing the meaning, simply to clean up. Then the team will be reviewing the initial report in its entirety, and that will be the time when we will try to catch all fleas in the text and then kill them.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARKLINS: What? You don’t like fleas?

UNIDENTIFIED MALE: [inaudible]

JANIS KARKLINS: Let’s now move down to the … I think it was Q, right?

MARIKA KONINGS: [inaudible]. Can I speak to this one?

JANIS KARKLINS: Please, Marika.

MARIKA KONINGS: Thanks, Janis. If we scroll to Q, right underneath that one we've added the language – if you scroll a little bit further down – that Chris has sent in relation to de-accreditation of identity providers. One thing we weren't clear on from the staff side is whether this language is intended to replace the de-accreditation of the accreditation authority. So there was discussion around if there's now a decision that [this] ICANN is not applicable because there are other sanctions in place … Or to remediate actions. Maybe de-accreditation is not relevant in that context. Or whether the idea was to have both of those sections basically together. Then, of course, you may want to review as well the language that Chris submitted.

JANIS KARKLINS: James?

JAMES: Thanks. Are you talking about Q still? Because you scrolled past it. If you could scroll—

JANIS KARKLINS: No. In-

JAMES: Oh, I see. The new language. Okay. So we've just essentially replaced "accreditation"—

JANIS KARKLINS: Yeah. The fundamental question is, do we still talk about de-accreditation of accreditation authority if we assume that the accreditation authority is ICANN? Or we speak about de-accreditation of identity providers instead of de-accreditation of ICANN as the authority. I think the logic would suggest that ICANN, as an accreditation authority, cannot be de-accredited because then the whole system is falling apart. There is an accountability system built in. If ICANN does something wrong, we can always remedy that through existing mechanisms within ICANN. But in reality we're talking about de-accreditation of identity providers if they follow the polices that are being adopted and that they need to follow.

Would that logic stand, James?

JAMES: Yes. I agree with that approach and I agree with that logic and I agree that, in this particular case, we no longer need to reference the de-accreditation of the accreditation authority because that is effectively the end of SSAD. So, yes, I think that works.

JANIS KARKLINS: Thank you. Marc Anderson?

MARC ANDERSON: Thank you, Janis. Sorry. I'm having a little bit of a side-bar conversation on that one. What Matt, Alan, and I were discussing was that ICANN may contract out to a third party to perform that function. We've allowed in our language that it might not be ICANN themselves. So we think it would still be worthwhile to have that language. So I think our quick side-bar consensus was that we would prefer to keep that language in there and then also have language for the third-party identity providers added. I don't think it hurts anything: keeping that language in there.

JANIS KARKLINS: Okay, thank you. Chris?

CHRIS LEWIS-EVANS: Sorry. I was just going to agree with exactly what Marc said. So he's covered my point. Thank you.

JANIS KARKLINS: Okay. Again, if we as a policy team assign ICANN to perform the function without clearly stating that they can outsource that function, can they still outsource the function? Again, I'm asking this because I do not know in reality how that functions within ICANN. Maybe that's a question to Dan. If we, as a policy team, suggest that ICANN should perform the accreditation function without specifying explicitly that we permit also that to be outsourced to the third party, can ICANN outsource still outsource to the third party?

MARIKA KONINGS: [inaudible] it says that they may outsource the function.

DAN HALLORAN: It would be a judgement call. I'd say probably we could if it's no prohibited. We could outsource it. We could get a vendor to help with that function.

JANIS KARKLINS: Okay. So then probably we should keep both, de-accreditation of the accrediting authority and de-accreditation of the identity provider.

Marc?

MARC ANDERSON: Thanks, Janis. If I may add to that, I believe this morning we discussed that very topic. Alex had a comment on that point, saying that ICANN could contract out to a third party. I believe Brian suggested that that be added as a footnote. So I think we have accounted for that scenario.

JANIS KARKLINS: Yes, you're right. You have a very good memory. Short-term memory, I would say.

Then we will keep both and we will review both texts, seeing whether we can agree with them. In the meantime, Hadia's hand is up.

HADIA ELMINIAWI: I do agree with the logic that, if ICANN actually delegates this to other parties, then we do need the accreditation part. But what if ICANN does not? So I think what we need to do is also put language there that makes it clear that we are talking about a case where there are other accreditation entities that were given that authority by ICANN. But just to keep it in there and then ending up with one accreditation entity which is ICANN and then having the possibility of de-accrediting ICANN – that's having the system fall apart – should not be an option, especially since I think it was in C where we put that the accreditation entity … I can't remember the language, but also it's responsible, I think, for the entity provider and the authentication provider. So, basically, if we get rid of "de-accredit this entity that's responsible for the two other elements of this system," we are ending up with no system.

JANIS KARKLINS: Okay. Let us move to the text. Then we will see. James, something to say?

JAMES: Just a note that I think somewhere in this document early on we said something like, "ICANN or its affiliates or its designees," and I just wonder if we should put that first and foremost wherever we refer to ICANN and this policy so that we are referring to that unless explicitly prohibiting ICANN from outsourcing that function, or something like that. That'll make it clearer when we don't have to clean up the whole thing.

JANIS KARKLINS: My suggestion would be to look in the text first. Thomas' hand is up.

THOMAS RICKERT: I was going in the same direction as James. I think something along the lines of "Where ICANN chooses to use a third party, measures need to be foreseen so that de-accreditation can be done for wrongdoing," or something like that.

JANIS KARKLINS: Again, let us look in the text and then we'll see. Now we will look in the text of de-accreditation. Let's go to Q first. We're talking about de-accreditation of the accrediting authority. We're explicitly suggesting that this would be applicable where ICANN outsourced this function. But then the question is whether the text is acceptable as it is now displayed on the screen with additions that are on the bottom.

Marika?

MARIKA KONINGS: We discussed earlier that the bracketed language -- I just realized that I didn't remove the second brackets, but I think in our current scenario, it would be, "If ICANN determines that the accreditation authority," then we should probably add in brackets something like, "which has been outsourced has materially breached," because I'm assuming, in this scenario we're talking about now, we're talking about de-accreditation of the outsource function by ICANN, and it would be

ICANN that would be overseeing that and de-accrediting the party to whom they outsourced that function if they believe that they're not meeting the requirements and have materially breached the conditions of the agreement.

JANIS KARKLINS: I have Alan's hand up. Alan Woods?

ALAN WOODS: Thank you. Just going to Hadia's point on that, if we leave it so that ICANN is the accreditation body, that removes accountability if there were to be an issue. Now, obviously, we're talking about this nuclear approach and that there'd have to be major wrongdoings. The likelihood of that occurring is low, but, if the same time, if we're creating a nice, robust policy, we should take into account the worst-type situations.

So I think we probably would need to figure out some way of holding ICANN – oh, God, it sounds terrible—accountable, should they misuse the power that is given to them. One of the ways I was just thinking of – I was trying to do a quick side-bar there – is potentially that ICANN can accredit some internal part of ICANN to be the accreditation body. Then, if that body is found to be deficient, it is up to ICANN to then fix it, basically.

[MARIKA KONINGS]: [inaudible]

ALAN WOODS: [inaudible]. So it's a difficult – again, very, very quick. But again, ICANN is to nominate an internal part of it or a section of ICANN itself to be that accreditation body in a way. [Then the] second one works again.

JANIS KARKLINS: We have a proverb which suggest that the deeper you're in the forest the more trees you have around you. I think we need to try to stay as simple as we can and as high-level as we can.

In any case, any unit or part of ICANN will be treated under ICANN accountability rules anyway because that is a part of ICANN. So, if the function is outsourced, then that entity is not part of ICANN, is not under the rules of ICANN and also the accountability framework of ICANN. As a result, these are different things. But let's try to be as pragmatic as simple as we can in this respect.

I have five requests, starting with Chris.

CHRIS LEWIS-EVANS: Thanks, Janis. I put some text in the chat box, replying to Hadia's point. Realistically what we're talking about is that, if ICANN is the single accrediting body and we get to the stage where we would be thinking of de-accreditation … Realistically, we got past all the compliance issues. ICANN should have sorted the small problems out because that's what the whole process if for. So we're now really talking about something that's happened that's caused a massive data breach or a

loss of personal data. We're talking about a really serious problem here. Realistically, the only thing that you can do after that is refer them to some data protection body, whichever one is the most relevant for that loss.

So I think that, for me, feels like the best catch-all for that nuclear option: they would almost self-refer themselves to the relevant data protection body.

JANIS KARKLINS: And do what?

CHRIS LEWIS-EVANS: Well, then they'll be fined and remedial actions will be put in place by a data protection body which then gets reassessed and they recheck it. It's all part of what they're there for. That's the role of a data protection body, really.

JANIS KARKLINS: Okay. Let me take Dan first. Dan, your hand is up.

DAN HALLORAN: Thanks. I'm still confused about the concept of accreditation authority. To me, if you're recognizing ICANN as the accreditation authority and you're talking about outsourcing it, that's just a vendor to ICANN. We would terminate that vendor relationship, but we're not really de-accrediting the accreditation authority because then we were the

accreditation authority. I think then we're talking about un-recognizing identity providers.

So I'm still lost on the concept of de-accrediting the accreditation authority if that is ICANN because it's circular to me. If you're talking about accountability of ICANN, we have accountability mechanisms already. We're accountable under the law. We're accountable under reconsideration, under our contracts with contracted parties. So I'm just confused by the concept. Just wanted to flag that.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. Part of what I was saying Dan covered. If it's indeed outsourced, it's contractual terms. All we really need is a statement saying ICANN has to be able to ensure the accountability or the reliability or whatever of whoever's doing the work. We don't need to write the contractual terms here. So I think we should put this as a principle – what ICANN needs to do at a high level – and not worry about wordsmithing it.

I feel in this discussion that I'm reliving the ICANN stewardship transition discussions of how to outsource IANA and make sure it's accountable or whatever. We ended up with an ungodly procedure there, and I don't really want to replicate that. So really we're looking to ensure the accountability and respecting our overall rules in doing this. I think that's as far as our policy needs to go.

JANIS KARKLINS: Thanks. Milton?

MILTON MUELLER: I share Alan's sense of déjà vu about the stewardship transition. Of course, in that case, the dodge of creating a so-called internal corporation of IANA was indeed an accountability dodge. But in this case, I don't think we have that problem. I think it's quite straightforward, which is that the GDPR is a law that ICANN must comply with. So, if their accreditation process is allowing people to abuse privacy rights, then they could be challenged under that law, I think, by almost anybody. Couldn't I as a data subject say, "I'm suing you, ICANN"? Or couldn't the data protection authorities bring a case against them? I'll ask the lawyers to answer that question, but my impression is that it would be. So I don't think we need to create wheels within wheels to hold ICANN accountable to be the accreditation authority. I think we simply need to enforce the GDPR.

JANIS KARKLINS: Thank you. Thomas followed by Marc Anderson.

THOMAS RICKERT: Thanks. You mentioned that you have the saying with the trees and the forest. There's another saying about broken records, and I feel like one every now and then. This is a point where it's so difficult to discuss an

individual aspect without having the compete picture, without seeing the entire policy.

Let's just assume for a second that we are at the point where we acknowledge that we have a joint controller scenario. What you would typically – that you can put into one sentence – is you would allocate the functional responsibility to take care of the accreditation to ICANN and also authorize ICANN to use agents or other third parties to conduct that to make sure that they play by the rules and kick them out if they don't play by the rules. Then you would add an additional layer and say, if ICANN fails to fulfill its functional responsibility adequately, you can reallocate that. I think that's all we need to say.

As much as I think that, for sanctioning, the approach that you mentioned, Chris – to refer them to the authorities – would work. But I think that we're not interested in getting any of the parties sanctioned. We want to make sure that, in case there's something wrong, the problem is fixed, that we make it work. I think, in that sense, we would just take this role away from ICANN and find somebody else to do the job.

Ultimately, it's enforcing and implementing the policy that we're just drafting. If we get the parameters right in the policy, we take ICANN to do that and we need to find a way to get somebody else to do it if ICANN can't do it.

JANIS KARKLINS: In Sub-Point C that we just adopted in the morning, we allocated that to ICANN. The accreditation policy defines a single accreditation authority run and managed by ICANN org, full stop. So that is our determination.

Now, in the case of Point Q, it's whether then we need to de-accredit the accredit the accreditation authority (alias: ICANN org) or not. Now, after this round of conversation, I am more inclined to say no. We even need not to say anything about performance because there are already safeguards in place for how we monitor and assess ICANN's performance in general terms. I would suggest that all we need is to define what would be the process of de-accreditation of the identity provider should the identity provider fail to perform a function or follow the policy. So, again, this is simply trying to think in logical but simple terms and not make much confusion.

Would that be something we could live with? In Point C, we agreed that the single accreditation authority will be run and managed by ICANN org. It means that ICANN org has all the safeguards in place in terms of the performance review by the community. If something will go sour, the community will say, "Careful."

As a result, we need not specify the de-accreditation of that authority that is ICANN. If ICANN will decide to outsource, then ICANN will still remain responsible and, as Dan suggested, would terminate a contract with the third party which would perform the function of the accreditation authority because the responsibility will stay with ICANN in any circumstance, right? So that means that we need to talk about

de-accreditation of the identity provider should the identity provider fail to perform functions according to policy. So that would be the logic.

Milton, please?

MILTON MUELLER: Just a clarifying point. It's not community accountability internal to ICANN that I'm not talking about here. I don't think that's what we can rely on. It's legal accountability to the DPAs or the GDPR or whatever law is applicable. We know that we tend to be divided on these access and disclosure policies, which means that internally there may be people within ICANN who will be perfectly happy if ICANN is sloppy and lax in its accreditation, and we would never possibly get something through the community. However, if they are in fact breaking the law, they can be brought to court. They can be sued. They can be fine. So I think we should specify that that's what we're relying on here, not the community.

JANIS KARKLINS: If I may ask to the overall hands – I have four of them in front of me … then the question is to please give suggestions on how to formulate that particular issue of the responsibility of ICANN or accountability of ICANN in performing the function [of the accredited entity]. How would that sound?

Milton, can you provide some idea, a simple formulation, on what you mean or how you see that?

MILTON MUELLER: [inaudible]?

JANIS KARKLINS: No. For the moment now, again, we're talking in conceptual terms. We are in agreement that ICANN org is the accreditation authority. So what's next? The accreditation authority or ICANN org, which is identical, is or should …

MILTON MUELLER: The accreditation authority should be compliant with applicable data protection law. If not, ICANN will be subject to fines. You could also have a community challenge mechanism that you could specify. So there's no reason not to try to do both. But I'm just saying the key issue here is whether they're compliant with law and not a self-reinforcing or self-enforcing kind of a thing.

JANIS KARKLINS: Okay. Now I have even more hands. Could you lower, please, all of them? I have Thomas, Marc, Alan, Milton, and Stephanie. Please take down them all. Now we're talking about how to formulate this question of the accountability of ICANN as the authority.

Alan Greenberg, please?

ALAN GREENBERG: As Milton said, we can invent a new accountability mechanism, but it is going to be subject to laws. Contracted parties are going to have a vested interest in making sure ICANN doesn't release information or give them accreditation information which ends up with them releasing information to people who aren't doing it legitimately.

So you've got a whole bunch of mechanisms that are going to be in place, all surrounding compliance with the law. I don't think we need to specify it in any more detail. We can note it but we can't invalidate the law. So I really don't think we need to go to any great pains about doing this. I like your formulation that we're saying we're not going to talk about de-accreditation of ICANN anymore. Again, déjà vu, but Thomas said something interesting. He said we will reassign it. Who's the "we" if ICANN is no longer in authority?

So I don't think we need a lot of words here. I think it's a relatively simple situation. It's compliance with the law and we need to simply refer to that. There's always going to be other challenges that various entities can evoke.

THOMAS RICKERT: That would be in the joint controller agreement. The joint controllers would reallocate the function of responsibility.

JANIS KARKLINS: Let me take Stephanie now.

STEPHANIE PERRIN: Let's be clear about what we're trying to do here. We're trying to decide what the ultimate recourse mechanism is in the event that ICANN messes up as the accreditation manager, as it were. At least some depends, in terms of liability, on whether that entity is a processor or a controller or a joint controller, as Thomas just indicated. That's going to set out your standards.

However, in my view, any entity that sets itself up in that vulnerable a role would be foolish not to have deep security controls to make sure that it was not messing up because your liability goes up with the amount of risk you're exposing everybody to because of your own sloppiness and bad management practices.

So that we could focus on, but whether that means a whole new accountability mechanism? I don't think so. We don't want to reinvent the wheel here, but we also don't want to force the Non-Commercial Stakeholder Group to start a little complaints-generation committee to keep ICANN honest. That wouldn't be a good outcome either, not just because the inherent loss of faith that you might have in us but because you're going to have liability if you wind up in court over these things.

So these are implementation issues, I think, that we ought to be sorting out at the implementation level. And it's good controls and also clarity about who's doing it.

JANIS KARKLINS: Thank you, Stephanie. Marc, are you in agreement to delete Q?

MARC ANDERSON: Thanks, Janis. I've been trying to get in to build on what Chris and Dan said. I thought Chris's suggestion in chat about recommending ICANN to the data protection authority was a good suggestion. I think that addressed the concerns. We're trying to build a system that as proper oversight and accountability yet still allows requests to continue to come through

Dan, I thought, made some real good points when he was talking about that, if you have a vendor that's not performing, ICANN is just going to terminate the contract. If there's an identity provider that's not doing their job right, then ICANN is going to stop recognizing the entity provider.

So I think we can use that. I think the combination of Chris's language and Dan's intervention gets us what we're trying to accomplish. It gets us accountability and oversight of the identity providers and any vendors that ICANN uses and puts in this principle that, if ICANN is not behaving, then ultimately the DPAs are responsible for enforcing that. So I think that's a way we can thread this particular needle.

JANIS KARKLINS: Okay. Marika?

MARIKA KONINGS: Thanks, Janis. My question is, is that something that needs to be spelled out here? Because it seems to be already part of … ICANN will establish an agreement and, if the agreement is broken, there are consequences. Similarly, the reference to the data protection authorities – I'm not sure

if we write in here that that is possible that otherwise is not possible. Or the other way around. So I'm just wondering because I think a lot of this is all about applicable laws and regulations as well as existing accountability mechanisms. I'm not sure if we need to call that out or whether that's already … because those are in place. So that's just a question.

So, in that sense, I think, as [inaudible] said, Q is probably not necessary. Maybe an overall statement, but that may apply to the whole package of recommendations, which could be that any and all applicable laws, as well as existing accountability mechanisms, are available to the relevant parties where these apply. I don't know if that is helpful to just reaffirm that, but it's presumably not something that is a policy recommendation because I don't think its in the remit of this group to change that.

JANIS KARKLINS: Thank you, Marika. Hadia will be the last one and then I will make a suggestion.

HADIA ELMINIAWI: Actually, I was going to say exactly what Marika said. I do agree with what Milton said, that ICANN should be subject to law, but ICANN is subject to law anyway, whether we say it or not. So why does it matter if we say ICANN should comply with GDPR? It doesn't matter if we say it or not.

Also, with regard to the contracts with whoever they authorize, also, whether we say it or not? Well, we don't need to say it. That's the thing.

Also, to Chris' point with regard to the DPA, well, that will happen anyway if a breach happens. So I don't know why we need to spell it out. Thank you. And, of course, yeah, we don't need Q.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Sorry to have another kick at this can, but I don't think I was clear enough. We need possibly a policy recommendation here that ICANN institutes sound management practices to deal with whatever you're going to call them because they're data processors. They're managing the accreditation of the folks that … And that's important to avoid liability.

I raised my hand because I'm not comfortable with what Marc Anderson was saying, that the law is there. You can't just leave it up to the law and the DPAs because that throws it into the hands of civil society to litigate. It's not up to the DPAs to launch their own complaints. They're there to adjudicate. The court is there to hear cases. ICANN needs to up its game.

Why I'm concerned is that it's had in the RAAs for years the whole concept about stopping scraping, data limiting for scraping, registrars getting paid for bulk data access. Have they ever policed that?

Apocryphal data says no. So I do think we need a reminder to up our game here. Thank you.

JANIS KARKLINS: Thank you. My suggestion would be the following: to replace Q with the new language that is based on Q. Then, somewhere in the overall description, we make a point that ICANN that would include not only sound management policies that Stephanie was talking about on accreditation but also including any other function that ICANN potentially would perform in SSAD in general, so that these sound management practices should be put in place in terms of execution of this policy. So I think that that is what we need to refer to and move on. Otherwise, we're spending too much time on this where we are more or less in agreement.

Would that be okay? Replacing Q with the new language referring to de-accreditation of identity providers? Then putting somewhere in chapeau one overall statement about sound management practices should be put in place to implement this policy as far as ICANN is concerned.

Farzaneh?

FARZANEH BADII: Thank you. I have been sending stuff to chat, but my concern is that, if ICANN does not put in place these sound management mechanisms, then it should be challenged. We need to somehow in our policy say how we can challenge it. It can be simply that we can go to the IRP or a

process like that to challenge it. I don't know how your suggestion actually addresses this concern.

Just because it's a déjà vu doesn't mean that it's not an important issue because people have been in this for the past 20 years. They've been discussing it. They might get a lot of deja vus. It doesn't mean that they're not important issues. I think we should flag this and discuss it a little bit more and not finalize it. Thanks.

JANIS KARKLINS: Thank you. Dan?

DAN HALLORAN: Thank you. Your approach sounds good to me. I'm just a little bit confused still. We're double-using the word "accreditation." We're accrediting identity providers and I guess the identity providers are accrediting users. Maybe there's a different word we can come up for what it is that ICANN does with identity providers, not "accrediting." "Recognizing," licensing," something, but not accreditation.

JANIS KARKLINS: Which line are you talking of?

DAN HALLORAN: The very first line. "The recognition policy for identity providers should include graduated penalties." I think it could be, "Recognize an identity provider," instead of "de-accrediting" them because –

UNIDENTIFIED FEMALE: [inaudible]

DAN HALLORAN: Hmm?

UNIDENTIFIED FEMALE: [inaudible].

DAN HALLORAN: We're talking ultimately about accredited users of this system, so it's still a little bit unclear to me who's doing exactly that accreditation. Is it the identity providers? Is it ICANN, the authority? So these would be ICANN-accredited SSAD users, basically.

JANIS KARKLINS: Ultimately, yes. The text now is on the screen. I hope that this is something we could live with. I ask staff to take a note on the overall chapeau of the policy, to put in a sentence or paragraph related to sound implementation mechanisms and, as Farzaneh said, also something about existing accountability mechanisms that could be used to challenge in case of underperformance or mis-performance or something like that. But existing. I think that that would be something we could live with. That phrase will appear in the overall initial report once we will get it. Then we will discuss it further.

So Q is gone. This is now replacing Q. We can go further to T. Alan Greenberg, your hand is up?

ALAN GREENBERG: Yeah. Thank you. I'm just raising a flag. I think we have something else that we have to add, but I'm not sure. We now have two kinds of credentials. We have identifier credential and authorization credentials. We're talking about decertifying the identity providers. Do we need another comparable phrase for the authorization credential providers? Just asking a question. I'm not sure. But just make sure. We may need it.

JANIS KARKLINS: Alex will answer you. Alex?

ALEX DEACON: I had assumed that the identity provider would be managing both the identity credential and the authorization credential. We could separate the function there, but again, for simplicity, in my definitions, last I looked, I had placed that function in the identity provider world.

ALAN GREENBERG: Maybe we need to define "identity provider" to make that clear.

ALEX DEACON: I think what I'm saying is – I'll look – my definition of identity provider says they also do the authorization credential.

JANIS KARKLINS: I ask to scroll up to definitions. Now they're on the screen.

ALAN GREENBERG: Sorry. I missed that.

JANIS KARKLINS: [inaudible]. So then let us go down to …

MARIKA KONINGS: Now the number has gone a bit off.

JANIS KARKLINS: Yeah. Now it is V. Used to be T, now it's V. After consultations, we came up with the text which potentially may find agreement that will not be restricted to the number of SSAD requests that cane be submitted at the time with the understanding that possible limitations of SSAD response capacity and speed may apply, except where the accredited organizations pose a demonstrable threat to SSAD. For further details, see Building Block G.

Volker?

VOLKER GREIMANN: Not going into the content. I think we've made our position there clear and I think this is better than what we had before. However, the linguistics of this now make the second part, starting with "except,"

seem to apply to the later part – i.e., the understanding of the limitations. I think taking that newly added language out of that sentence and adding a secondary sentence to that might provide some clarity.

JANIS KARKLINS: So would you …

VOLKER GREIMANN: Basically I'm saying leave the sentence where it is and take the inserted sentence [out] the secondary sentence that begins after "SSAD." "It is understood that possible limitations to SSAD response capacity and speed may apply."

JANIS KARKLINS: That already is linguistics, and none of us are native English speakers, as I understand, Volker. So I think it does not change. I have no issue with that: putting it as a separate sentence, starting with "It is understood." That is exactly the same thing. But I would leave it to the staff to decide (some of the more native English speakers).

May I take that V is something we can live with?

Alan? Please say yes.

ALAN GREENBERG: Yeah. Just noting the word "organization" is probably the wrong word there.

JANIS KARKLINS: It is.

ALAN GREENBERG: "Accredited organization." It may be an individual.

UNIDENTIFIED FEMALE: "Entities."

JANIS KARKLINS: "Entities." Okay, so let's see whether – Dan?

DAN HALLORAN: Two notes, one from an implementation point of view. I think org can live with this, but it's much clearer for us if the requirements say who must do what. This is stuck in the "accredited organizations or individuals" and says "they will not be restricted." By who it's unclear. Who must do what to make this come to reality? What's the operative restriction? So someone can in the implementation can go back and try to guess what this means, but it would be clearer – like if it said "in the gateway." "The gateway must not restrict accredited organizations except for the following." So I think it's a little bit in the wrong place and a little bit [inaudible] reword it could be better.

One other note. I'm still a little caught on "entity." It's confusing to me. Again, we can learn to live with it. But, to me, an entity is usually an organization, not an individual person. So you talk about persons or

organizations. Persons [are] entities. But now we're using, if I understand right, entities that could be a person or an individual. I think it might be a little confusing trying to translate that back into everyday usage. Thank you.

JANIS KARKLINS: I think, in relation to this sub-point, we had a conversation where some said that maybe that does not belong exactly in this place. I recall that my answer was, "Let's try to agree in principle and see whether the placement of the principle is right or not." So what I would say is that, once every block will be finalized, we will put them in order. Then we will do logical reading, and then we can shift agreed text back and forth around, making sure that they're placed in the right order and that they read in the right sequence.

Answering your question, maybe we need to think – again purely technical – adding further in the text a reference that entities means accredited organizations and individuals. Then at least that gives an explanation of what we're talking about.

I hope staff is taking notes and will do the homework on those.

Let's then see – scroll down. We had a bit of a hiccup and inconsistency in the part of auditing and logging by the accrediting authority and identity providers. Since this part of the auditing and logging specifically refers to accreditation, it was not properly worded at the beginning. So, at lunchtime, staff made some editorial suggestions that

now are displayed on the screen. Again, this part is purely about the auditing and logging of the accreditation process, not requests, per se.

The suggestion is to formulate the first sentence. "The accreditation activity of the accreditation authority and the identity providers will be logged by those parties."

Volker, your hand is up.

No? The next point: "Logged data will remain confidential by default and will be revealed under legal justification. Logged data will be retained in accordance with applicable law."

Volker, it was your [hand]?

VOLKER GREIMANN: I'm just a little bit unclear on two parts. Confidential from whom? The second part is what we mean by legal justifications. That's pretty unclear language. So I would like to see some more explanation of those two terms.

JANIS KARKLINS: Okay. Thank you for your questions. Farzaneh?

FARZANEH BADII: My question is, now that you said that this is not about queries but about the activities of the accreditation authority and identity providers – I don't know if my comment is actually correct here but I'm going to make it anyway. … Basically, sometimes the confidentiality of

the requests can prevent individual auditing and knowing how many request and queries have been undertaken by, for example, law enforcement and other entities and how this system has been used. Such confidentiality would impede the transparency of the request in general. We have seen problems with, for example, social media platforms in the reporting of the queries of law enforcement because they want to keep it confidential.

I'm not saying that it should not be confidential, but I think that there has to be some kind of provision that, later on, some queries be unsealed or there's some information that can be not identifiable queries. But certain information for transparency reasons should be issued and should not be kept confidential. Thank you.

JANIS KARKLINS: We have a logging block which will address the logging information about queries. So here we're talking explicitly on how to maintain information about accreditation. So that does not entail any logging of any queries for the moment.

Alex?

ALEX DEACON: I'd always presumed, perhaps incorrectly, that the auditor, in order to audit the system, would need access to some logs to do that properly. If that's the case, I'm wondering if this would prevent the auditor from doing their job. Do we need to allow for that?

JANIS KARKLINS: No, I think that Sub-Point E allows auditors to access data.

ALEX DEACON: Okay. I didn't read that far. But …

UNIDENTIFIED MALE: [inaudible] or the legal [inaudible]

JANIS KARKLINS: The question that Volker raised should remain confidential from whom or for whom. Then there was a question about legal justification.

Marika, can you speak on those?

MARIKA KONINGS: I don't think I can. I'm trying to remember where this language was taken from. I'm looking at Margie's. Is this potentially coming from the BC input on accreditation originally? Because I think we took some stuff from there. So I don't know if Margie can maybe answer the question.

JANIS KARKLINS: Margie? All eyes on you now.

MARGIE MILAM: Just give me a few minutes. Let me look.

I think we were talking about having the logs available obviously for auditing – I mean, that makes sense – and then subject to court order is probably legal justification means.

JANIS KARKLINS: Yes, please, Farzaneh?

FARZANEH BADII: Thank you. Just a clarifying question. Sorry. I'm a little bit confused. When we talk about accreditation activity and logged data, what do we mean exactly? What are we talking about?

JANIS KARKLINS: I think the implementation phase will determine which data should be kept as logged data – when it was submitted and by whom. Probably that is the first thing that comes to mind.

Margie?

MARGIE MILAM: Thank you. I found some more information. I had put, "Logged data would remain confidential by default and can be revealed only under legal justifications because revelation could, for example, compromise law enforcement investigations. Logs should be further available for data protection authorities and ICANN for auditing." So I think that's what we were thinking about.

UNIDENTIFIED MALE: Yeah.

JANIS KARKLINS: Okay, but that sounds to me more like the logging of requests of disclosure. Let me collect a few comments now. I have Milton, Volker, and Matthew in line. And Alex.

MILTON MUELLER: Let's focus on the question that Farzaneh, which is, what are we talking about? What data here? We're not talking about the queries. We're talking about the entity, essentially, of the accredited parties. So I think that this is not adequate: to have that information only revealed by a court order. I think we actually need to create a system of standardized access and disclosure for getting access to this accreditation data. I think that we could prolong the joy of this working group for another year or two if we created that because they are users of the Internet infrastructure and they have to be publicly accountable.

No, I'm just kidding, but I do think we could actually do away with such in D completely, except maybe for the sentence, "Logged data will be retained in accordance with applicable law." We don't need to say anything about that because E, by implication, means that you're not publishing this data but you are clearly making it available to examination by the accreditation authority or the independent auditor. I don't think we need to say anything about court orders or confidentiality by default.

JANIS KARKLINS: Thank you for your suggestions. So that would mean the text which is now outlined would go. There would be only "Logged data will be retained in accordance with applicable law," and then the E section.

Volker?

VOLKER GREIMANN: Thank you. I'm very sympathetic to the suggestion of Milton. I think there would be a certain imbalance of the requesting parties for data would only have to provide a legal basis for their request, but the person that wants to know who requested the data would have to provide a court order. That would be a certain imbalance there that I think I have a bit of a bad feeling in my stomach with. I think, by removing that, that would be a good idea.

However, we could also flip this on its head and say, "In case of a court order or a legal basis is provided for requesting anonymity or confidentiality of that data, that option should be available." In that case, the data could be declared confidential by the party making that request. I think that will still take care of the interests of the requesting party that has an interest in certain confidentiality if they have a legal basis for that. So, if we flip that on its head, that might be workable and might be a solution for all parties.

JANIS KARKLINS: Thank you, but isn't that the last sentence? "Logged data will be retained in accordance with applicable law?" Does it? Because it fully covers that concern.

Let me take Matthew.

MATTHEW CROSSMAN: I agree that I think the language as is is probably fine and we can probably work on the details and implementation, but I think, to answer's Farzaneh's question, what we're probably talking about is that these parties should be able to demonstrate the information they relied upon in making the decision. I don't know if it would be helpful to the implementation team to include some language along those lines. Maybe we can add that. I think, at least in my mind, that's where we're talking about when we say "accreditation activity."

JANIS KARKLINS: Thank you. Dan, your hand is up.

DAN HALLORAN: Thank you, Janis. One implementation question is coming to mind, and I'm not sure if I've gleaned what the understanding of the team is: if the fact of accreditation of the users will be public or not. For example, ICANN currently publishes a list of all ICANN-accredited registrars on the website. Is ICANN supposed to be publishing a list of all ICANN-accredited users, or will that be confidential – the fact that someone is an accredited user or not? This accreditation information and the logging is going to include personal data, which is going to have its own GDPR implications. Especially if people are accredited users, we're going to have to respect their personal data rights and there'll be personal data mixed in with the accredited organization data, too. Just

something to keep in mind in terms of who has access to that and how long we retain it and stuff.

Last one. Now that we're looking at this auditing of accreditation authority and now that we've put in ICANN as the accreditation authority, I haven't thought through it a lot but it raises new questions to me. Basically it would be ICANN paying for its own independent audit of its own function and then responding to that audit is going to seem like it's going to be pretty expensive and possible burdensome to be paying for that audit. Responding to that audit is going to be burdensome on the people who are implementing the accreditation. I can't think of another parallel like that, where we have independent auditors reviewing other ICANN functions, aside from audited finance, but that's an expensive, burdensome process.

So just a few issues with the auditing, independent auditing, whether or not it's confidential –the accreditation – and then the need to respect the personal data rights of the people who are being accredited here. Thanks.

JANIS KARKLINS: All things in ICANN seems to be so complicated.

DAN HALLORAN: Was that about trees and forests?

JANIS KARKLINS: Indeed. We have now a few questions on the table. They are more, of course, of an implementation nature. Any reactions? I don't know how many hands there are. I think Volker and Dan's hands are old. Alex?

ALEX DEACON: There's been questions about what exactly is going to be logged here. I think Matthew is right. I think the one set of information that would be logged, as he mentioned, is the incoming request for accreditation, which is the information that the requester is providing to the accreditation authority before being approved and issues a credential.

Then other set of information, which I put in the chat [on] logging information which I think will also be interesting and important for the accreditation authority and the identity provider is that, whenever that credential is used, that credential is presented, in the case of a gateway, to an identity provider to be validated to ensure it still hasn't been revoked and it's still valid for use. So I believe that will also be logged, which will be important information to keep so it could be checked if necessary. Thanks.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: Regarding the data to be logged, we had suggested the accredited entity, the purpose, the query, and the date for data fields. That seemed reasonable.

JANIS KARKLINS: Yeah, but for this, we're not talking about the query itself. We're talking about accreditation in this part.

MARGIE MILAM: Got it.

JANIS KARKLINS: So query will come in another place. Chris?

CHRIS LEWIS-EVANS: Thanks. I'll take a stab at answering Daniel's first question, I think. Me and James actually discussed this when we were talking about the confidentiality level of law enforcement requests. Under GDPR, it's obviously very important for the data subject to know what personal data is being processed and how that data is being processed. Really there's an expectation of that, if this data is being processed by third parties, then those data subjects need to be known. What sort of third parties are processing their information?

So going to the question that Daniel posed, would it be a list of A, B, C, D, E, F, G? I don't think so. I don't think we need to cover that under GDPR, that you have to list every single entity that could process your data. But certainly the sort of groups that they fall into would have to be detailed and would have to be made visible to the data subjects,

whether it's on the SSAD system and/or [must]. Also on the contracted parties as well. Thanks.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: I think Dan has raised a number of very interesting questions as the privacy officer for ICANN, but it's a good exercise for this distinction between legal persons and natural persons. It'll be interesting to see how many of the cybersecurity researchers identify themselves as legal persons and how many identify as individuals. In terms of transparency reports that are required under GDPR, that would be a separate issue. And they might not just be required under the GDPR. They might be required separately under national and provincial, in this case of Canada, or state law, a state being a sub-section of countries. So that's the transparency reports.

Then there's the issue about whether ICANN as a fully transparent organization should have a list of accredited entities. I don't mean the casual one-offs. I mean the regular accredited entities above a certain volume. I see that as another implementation issue, but it's a sound management practice issue that we have to iron out at that stage at least. But that's an important distinction: what we have to give the individual under data protection law subsequent to the request and what we do as a transparency. Thanks.

JANIS KARKLINS: Listening to this conversation, I'm wondering whether we're, again, not digging a hole for ourselves. There are many systems or many activities in the world which are used by many people, and not necessarily all those systems publish who are the users. So here as well. If there will be requests specifically to ICANN or a question of whether that entity or that individual are accredited, then you will answer after examining whether that does not fall under GDPR. But, otherwise, the system will run. So I'm thinking of how many banks are listing all their clients in public. But there are millions of clients, probably. The same here. So, if we want to contemplate, we can ask those hypothetical questions. The reality is that we need to follow, as much as possible, the common sense and unusual practice.

I have Alan Woods and then I will try to make a proposal.

ALAN WOODS: Thank you. Just two very brief comments. One is I completely and whole-heartedly agree with what Chris was saying there. There is not, to dare use the word from Phase 1, purpose, really, that I can even see for listing all the accredited users. In fact, I think it would be hard to actually point that out. So I think that ICANN has that list, obviously. They need to know who the accredited people are. [That's] good enough. Then we go onto them as controller for that. We'd need to deal with that.

My second point – I put into the chat a little bit earlier – is that why we need to have these logs, obviously, is the subtle change that came about in GDPR. I know I'm not limiting myself here. Instead of being

compliant, you have to show compliance. It's as simple as that: they need to maintain that accreditation, the act of accreditation, was done, considering certain things, and that log should represent a repository of the decision that was made, as in, "Why did you come to that decision? Why was it accredited? What did you get?" Then, only if there was a question raised as to the validity of that accreditation should that data be released in order to show compliance.

I just added in the potential rewording on that, again limiting it to where it was a legal obligation of other the accrediting entity or the identity provider or then where there is an audit, as is contemplated under the policy that we're trying to come up with. So I tried to make it that way just to see where my brain is going in this, but I think there is good benefits. We can actually quantify the benefit of why we need logging in that.

JANIS KARKLINS: Thank you. I think that this is almost the end of the work on the accreditation building block. We need maybe to take a look to your suggestion in the chat that I cannot see. My proposal would be the following. Now we will stop discussing this. Staff will try to reformulate the text based on conversation and submissions that we have. Most likely in Point D the first sentence will go. Then a few other edits will be provided. We will look at this specific point at the very end of today.

Now we have about 20 minutes from break. I would like to see whether Rafik would be willing to take 20 minutes to discuss the issue that the

council raised, which you asked me to give you some time in the team to do. Sorry that I'm putting you on the spot immediately.

RAFIK DAMMAK: Can I start?

JANIS KARKLINS: Yes, please.

RAFIK DAMMAK: Okay.

JANIS KARKLINS: And you can use my Zoom for it and identify – please take all hands down now.

RAFIK DAMMAK: Already I see three hands before starting. I sent this week the letter to follow up an action item from the council meeting last week. This is in relation to consultation on Recommendation #12. Basically, the suggestion here is to provide an implementation guidance based on what we got from the Board letter, where they highlighted their concern and were giving an example of what we can have there.

I know that there was already some reaction to my e-mail. I can say there is support to what is suggested as a path. I would like to see if there is any other reaction because I would like to bring back the initial

feedback from the EPDP team to the council tomorrow so that it help us at the GNSO Council level to work on the response to the Board and also to reach closure of this issue.

Checking the queue, I see we have Hadia and then Alan.

HADIA ELMINIAWI: Thank you, Rafik, for sharing the information with us. So your suggestion is mainly to take this issue to the implementation guide and not deal with it in the policy phase and also to keep Recommendation 12 as is with the two options of redaction and deletion, right?

So, if this is actually your proposal, I don't agree with it because – or we don't agree with it – this is actually a policy issue and not an implementation issue because, if you believe the deletion option there, that means that there could be a possible negative impact on registrants. If you remember, when we actually made this recommendation, it was a compromise. Back then, we did agree to having both options – deletion and redaction – because we did not foresee the possible negative impact on registrants.

Having said so, there is not clear logical reason behind having the deletion option. The redaction option is already there. What's the clear reason for having the deletion option? As I said, when we agreed, there was no clear reason for us back then as well, but it was a kind of compromise.

So my suggestion would be to delete the deletion option from the recommendation. And it's so simple. As simple as that. Thank you. So we do not support your suggestion. Thank you.

RAFIK DAMMAK: Thanks, Hadia. We have Alan Greenberg, and then Marika, James, and Marc.

ALAN GREENBERG: Thank you very much. If you remember, that whole recommendation was made at a very late time in a meeting, and there was strong incentive for "Let get this closed so we can go home," essentially. All right, not everyone remembers it that way.

UNIDENTIFIED FEMALE: [inaudible]

ALAN GREENBERG: I believe, now that it has been raised by the Board as an issue, it is something we must reconsider. My personal belief is we should figure out a way to ask the registrants and make sure we have an answer or say the default is to keep the organization field. If that is not indeed possible or something this group is willing to reconsider, then I agree with Hadia that the deletion option, which, remember, was at the discretion of the registrar to delete, is losing information which could be valuable and could be important. The only rationale for deletion that

I have seen is there may not be a mechanism to convey the redaction to the registry if the information is passed.

However, we have other requirements throughout the policy that say, for instance, a registrant should be able to specify to the registrar that they don't want their information redacted and that has to be conveyed to the registry. And there was a timeline – rather [a specific] timeline, if I remember correctly – that said registrars would have time to be able to implement this. It didn't have to be done immediately.

I believe this one can be done in the same way. That is, if the registrar cannot confirm with the registrant that the organizational field should be kept, it should be physically kept at then registrar and redacted until such time as there is a definitive answer but it not be deleted from the information which can be revealed on a disclosure request. Deletion means it's not available for the disclosure request afterwards. So I believe that information should not be deleted but redacted and way is found to make sure that that is passed on to the registry if necessary, just like we are doing with a number of other optional redaction requests. Thank you.

RAFIK DAMMAK: Thanks, Alan. We have Marika, James, Marc, and then Milton. Marika, please go ahead.

MARIKA KONINGS: Thanks, Rafik. I just wanted to clarify or remind people where things stand in the process and what the council is expected to do here.

Indeed, the Board did not adopt the specific part in relation to the deletion of Recommendation 12. So that went to the GNSO Council for what I think we refer to as a consultation process. The council had various conversations with this group as well, with the Board.

What is ultimately expected to happen is for the council to either affirm or modify its recommendation in the form of a supplemental recommendation. That would need to go through the council as well with a similar voting threshold, a super majority vote, as the original recommendation in order to pass or have the same binding result on the Board consideration, who may still redact it or not adopt it if they meet the applicable thresholds.

So there is no specific guidance in the process and what the role of the PDP working group is that originally developed those recommendations. Of course, it's a bit of an unusual circumstance that the PDP is still information because, in most cases, the group will have finalized. So the council has indeed reached out to get the group's input on that.

So I think that's a bit where we are in the process. So it's really the council that will need to decide whether or not to modify the recommendation or supplement it in some way. I think some suggestions have been made and there could be a supplemental guidance on how this is excepted to be implemented to avoid the unintended consequences that I think the Board has described. So I think that's where we're at. I'll hand it back to Rafik.

RAFIK DAMMAK: Thanks, Marika, for the explanation in terms of process. Yes, here we are in a situation where the council is consulting the EPDP, but at the end of the day, it's up to the council to make a decision and to follow up with the Board.

We have quite a long queue here. James, Brian, Volker, Margie, and Alan Greenberg.

JAMES: Thanks, Rafik. Yes, I'm also now having my first run-in with déjà vu because it was also a meeting in Canada where we were discussing this topic at length. I don't know if it was the last day. I know we spent several hours on that topic.

I just want to say at the outset is that I think that the approach that was put before the council is the right approach. We're talking about making a fundamental change to the registrant organization field and injecting it with meaning that it has not had up until this time. That's fine going forward. I think we can all put together a logic process that captures the intent of the registrant from here on out.

The problem is that we have 130+ million potential registrations in a legacy database. If 20 or 25% percent of them have some data in the registrant org field, now we're talking about a population of domain names that's much in excess of the population of Canada. If we were to send each of them an e-mail asking them to correct and confirm that and we got a 90%+ rate of response, that still leaves millions of domain names that now have bad data in the org field and that are being

treated differently than they were when they created that. So it's really about addressing a legacy problem.

I want to be clear to council, council liaison, and Board members. When we talk about deleting data in the registrant org field, the registrar still has the data. It's not going away. It's not disappearing. We still have it. What we're saying is, if we're going to give that field new meaning, we have to give folks who may have inadvertently used that field a fresh start. We have to be able to hit the reset button on that field and give the folks the opportunity to use it in this new fashion. Otherwise, we don't know how many erroneous entries we have in there and we can't trust that field. The data in that field now becomes suspect, whether it's disclosed or redacted.

So I don't understand the concern here: if we redact or delete it. The registrar still has it. It's really about capturing the registrant's intent because we're changing the rules halfway through the game here and we need to make sure we understand that. We've seen, with renewal notices and transfer changes and all other kinds of policy messages that, if we get a 5 or 10% acknowledgement rate, we are thrilled because those e-mails mostly go ignored.

So that's the intent behind this. I think we have a sound process. I think that the recommendations from council are the most practical. It's not perfect, but it's going to get us there. And I think we have an approach. Thanks.

RAFIK DAMMAK: Thanks, James. Milton?

MILTON MUELLER: Not much to add to that. I support the council approach and I think we don't want to unwind and reset this carefully-though-through compromise that was worked out in Toronto. I really don't want to go there. Thank you.

RAFIK DAMMAK: Thanks, Milton. Next, Brian.

BRIAN: Thanks, Rafik. I think some of our frustrations/conversation comes from if you consider what to do about the org field to be on a spectrum of the rainbow, where red looks like allowing the deletion of the data and purple looks like what we would consider a common-sense approach of "This is the org field data and it shouldn't be personal data, so publish it."

In the middle there lies a lot of things that we could do. There's a lot of notice requirements or notice opportunities. There are things like including the note in this year's WHOIS data reminder policy e-mail that goes out. We could require a special e-mail to go out to registrants and inform them about this change and what's going to happen with this data. There's different places along this spectrum where we would land as far as what you do if you do or don't hear back. If you don't hear back, then you can go ahead and redact. Or if you do hear back, then you an

opt in because it's common sense. It's an org field. It shouldn't be personal data. Or the alternative.

So there's a lot of area in that spectrum. The fact that we landed on red or whichever way I just said it was is really frustrating. We would accept pretty much anything except for the outcome that allows for deletion. So take a step toward orange. Take a step toward indigo. Meet us somewhere that doesn't allow for the deletion of the data, which we all agree is important and really I think common sense tell you is very minimally risky to published. This is a field called the org field. This is data that the registrant gave you at one point, presumably, and has been reminded about every single year since then: to update this and make sure it's accurate. The risk profile for a registrant publishing that data should be really minimal. So take a step toward the middle of the spectrum and meet us there.

RAFIK DAMMAK: Thanks, Brian. Margie?

MARGIE MILAM: I was going to say something along the lines of what Brian was saying. There always has been a WHOIS accuracy requirement, so the org field should have been accurate and those data reminder notices every year reminded the registrant that it needed to be accurate. So I agree fully with my colleague and with the ALAC folks that the data shouldn't be deleted but something shy of that is what I think would be preferable. Thank you.

RAFIK DAMMAK: Thanks, Margie. We have Alan, Mark Sv, Marc Anderson, Volker, and James. I'm checking here with Janis for if we have to cut the queue.

UNIDENTIFIED SPEAKER: [inaudible]

RAFIK DAMMAK: [Dan?]

JANIS KARKLINS: Yeah.

RAFIK DAMMAK: Okay. Five minutes, so I ask everyone just to be brief here. Alan?

ALAN GREENBERG: Thank you. I think I heard Marika say that the council consulted with this group. I don't think that's the case. They certainly consulted with some members of the council who were EPDP, but not with the group as a whole. At least I was never consulted.

All right. The other option, Rafik, is to remand to the EPDP. The council doesn't have to make its own decision. It could remand to the EPDP, which is still operating to decide whether to change the policy or not. I'm just noting that.

James said that the organization field is suspect. Every field is suspect. We know there are significant accuracy problems and we don't necessarily know that anything is right. James also said that, if the WHOIS organization field is deleted, the information is still kept by the registrar.

Now, we've been told time and time again that your information about your client is separate from the WHOIS information. I've seen absolutely no basis for believing that every registrar who deleted that field in WHOIS will be keeping a private copy. I don't see a requirement to do that, and it certainly wouldn't be released if someone makes a valid GDPR request for information, which will give personal information but won't give the organization field. So, if it's deleted, it's information that is potentially lost forever, except in the domain names database, which we don't want to talk about. Sorry, that w as a joke. To delete information which may have value and to not provide it to someone who has a valid legal reason for getting the personal information about that domain registrant I believe is improper. I believe there's mechanisms to go around it. Remember, we have made this an option of the registrar. So I believe we have to remove the deletion option from the registrar. Redact it if necessary but don't delete. Thank you.

RAFIK DAMMAK: Thanks, Alan. Mark Sv?

MARK SVANCAREK: My first question was similar to Alan G's. When is deleted not deleted? Because I thought that this was data that was being kept separate and, if was deleted from the WHOIS record [or] the RDS, it would be deleted everywhere and there was no obligation do otherwise. So when I read "deleted" I was reading it as gone forever, irrecoverable, etc.

I also remember that, when we made this compromise – I was an advocate for this compromise, so let's be clear about that – we felt like it was perhaps an opportunity to create some sort of a data basis for trusting the org field as part of a natural/legal person distinction. If we're going to do that, it does need to be high quality data so that that argues in favor of sending out the notices, asking people to update them, and stuff like that. But we always knew that there were a bunch or risks, namely that some people use the org field as their registrant name, effectively. Then they just have a role-specific e-mail address, something like domain operator as the registrant, whereas the real registration is in the org field. So there was always a risk that deleting this was going to lead to unidentifiable registrants.

So that's the way I remember this compromise, which, again, I was an advocate for. I would like some clarity on what "deleted" actually means. I need some more coffee, I'm afraid. Thank you.

RAFIK DAMMAK: Thanks, Mark. We are just a few minutes away from the coffee. So I'm cutting the queue here with Farzaneh. Marc Anderson, Volker, James, and Farzaneh.

MARC ANDERSON: Thanks, Rafik. I'll just say real quick that I think the Board identified a concern. They provided an example and they provided a possible solution. The GSNO Council seems amenable to that solution. On behalf of registries, we're supportive of the GNSO Council's proposal. Thank you.

RAFIK DAMMAK: Thanks, Marc. Volker?

VOLKER GREIMANN: I'm a bit shocked at the ease of some members of this group to walk back certain recommendations that were made in consensus and suddenly no longer stand by the consensus that has been achieved in the past.

This is not a tool that we would like to use very often. This is something that registrars see that is a tool that is sparingly used. Data quality, especially in the organization field, has been abysmal for various reasons. We have resellers all across the world who implement this in different ways. Some require something to put in that field because they don't know better even though we tell them. So everybody puts their own name in that field. Sometimes it's just badly translated. We have about an 80% repetition rate of personal information in the name fields in the organization field, for example, for registrations coming from Japan. We see a lot of abuse of that field, or, let's say, misuse of that field. The ability to finally clean that about would be very much

appreciated by registrars because that field wrongly used caused issues for us as well.

We had reached this as a consensus, and we are happy to adjust that consensus in accordance to what the Board suggested. However, we are not walking this back.

RAFIK DAMMAK: Thanks, Volker. James?

JAMES: Hey, Rafik. Rather than come across as argumentative, I really, truly, and sincerely want to try to help here because I think we're going in circles.

I want to go to Brian's statements and some of the previous speakers'. Brian described a process – in the middle, he called it, of the spectrum – where we would try to notify a registrant. We would try to explain the changes to registrant org field, get them to take some action, but if they failed to take some action or we were unclear that we would default to some action where it would be deletion, he felt like that was not on the edge of the extremes of the [inaudible]. That's exactly what the recommendation says we should do.

So I guess I feel like, Brian, you're agreeing with us. Deletion was never a blanket. It was at the end of a failed process of notification and confirmation and taking action, but we wanted there to be this drain at the bottom of the pool who catch the folks who just ignored all of that.

To Alan Greenberg's point, whether or not you could trust the registrants to recover or retain this information is exactly what the council is directing them to do in this. It was designed not to hide information behind court order. If the org field is deleted, it is equivalent to it having never been there in the first place. So it wouldn't be accessible through SSAD or other means because it should not have ever existed. It is resetting the clock to what we expected it to be in that field, which is empty.

So I just want to point out then that the specific concern of the Board – I think Marc Anderson mentioned this – is, if we did this, we would not be able to recover ownership, that we would lose the link or chain of ownership of the domain name to the registrant. That was one possible unforeseen consequences. The guidance from the council addresses that and I think closes that vulnerability, that loophole. That's why I think we're supporting it. But I think we need to be very, very careful about letting the world as we wish it to be get in the way of the world that we have and the data that is in front of us that we're trying to work with, that we're trying to fix. This is hundreds of millions of records. Please think at scale. This information – someone mentioned the WHOIS data reminder policy. Single-digit percentage viewed, opened, and acted upon. We're talking about 90%+ of those being ignored or caught in spam filters. So this the problem that we're facing. I think we designed a not bulletproof but a workable solution, where deletion of the data is the caboose on that whole process, not the first step but the default step. But there's still a way to piece it all back together in case we have to.

So I hope that helps because I really am trying to take the concerns and say we have an answer for them. I feel like, if there are still concerns, then please the express the new thing that I have missed. Or maybe we're not hearing the actual concern.

RAFIK DAMMAK: Thanks, James. We have Farzaneh.

FARZANEH BADII: Thank you, Rafik. I just wanted to raise this point. I've been wanting to raise this point since the Board came up with this resolution and did not agree with Recommendation #12. It doesn't add to the conversation much, but I do not agree with the rationale of the Board that says in its resolution that the implementation of Recommendation 12 may result in the loss of the ability to identify the registrant. It is my impression that the WHOIS was never there to identify the registrant in the first place. I think it's very dangerous to say that and see this in the resolution. So I do not agree with that rationale, and I think the Board might want to correct itself in saying that.

I agree with the council recommendation, and I think what James said is quite reasonable. We have not heard any more concern that we can actually address. Thanks.

RAFIK DAMMAK: Thanks, Farzaneh. I cut the queue after you, but I see Thomas and Brian. So I guess we can give you the opportunity to speak, but that's it. I think

we cannot take more since we are already in the coffee break time. Thomas?

THOMAS RICKERT: I think I'm not really a friend of reopening consensus positions that have been determined. This is difficult enough. I think that, although we were exhausted when we last met, Alan, these were conscious decisions that we made at the time.

I'm interested in finding out what the motivation for reopening this is. If it is to have the data for publication at some point, I think that's not a good idea because we're giving all this a fresh start. If the motivation is for the rare instances where we need that data in order to make a link between a registrant and the domain name – i.e., to protect the rights of the registered name holders – then a potential way forward would be to request the contracted parties to block that data. There's a concept in GDPR whereby you make data in inaccessible from live systems. So it would be blocked. It can't be used. Even staff with registrars can't see that data. It would only be accessible for the specific purpose of where there's a complaint by somebody who says that he or she owns a domain name and they can't evidence that because the record has not shown in the WHOIS data or registration data in the registrars' live systems.

RAFIK DAMMAK: Thanks, Thomas. Brian?

BRIAN: Thanks, Rafik. Just to clarify my point there, where would be okay with landing is at the end of that process if the data were to be redacted at the end. To James' point, as you mentioned, if you want to go through the process of reaching out to the registrant again and you expect worse than a 95% open rate or read rate, then you can delete the data afterwards. There's no meaningful difference between that and just deleting the data right now.

So this needs to end in a place where the data is just redacted for all the reasons that I mentioned before. I'm sorry if I misspoke on what the acceptable outcome would be at the end of that process. Thanks.

RAFIK DAMMAK: Thanks, all, for all your comments. I think the initial feedback we can share with the council. We have already the thread on the mailing list. We're report this initial feedback, and probably the discussion will continue.

I think that we have Keith here in the audience. [No?] [inaudible] Okay. So that's it from me.

JANIS KARKLINS: Thank you. We have carved ten minutes in the coffee break, so I will give them back to you. Please be back in the room by 3:45. We will then try to finalize the accreditation building block with the last bit that we discussed, and then we will move on to the acceptable use building block. So a 15-minute break – sorry, I said 3:25. Sorry. 3:25. 15 minutes.

May I call the meeting to order? With this number of team members around the table, we can finish work very quickly.

May I ask team members to come to the table? Back to work. I think we can start recording. Let us continue consideration of the accreditation building block. I mentioned at the end of the previous session that we would revisit the only remaining piece that we need to look at. The staff made a proposal based on the conversation that we had. They captured those elements. The captured elements now are displayed on the screen. I think on Sub-Point C we were already in agreement. Mostly we're … no, sorry. We need to look at both, yeah.

On C, the suggested language is now as described on the screen: the accreditation/verification activity, and then listing, not exhaustive, such as accreditation request information on the basis on which the decision to accredit or verify the identity will be logged by the accreditation authority and identity providers. Then the logged data shall be disclosed or made otherwise available for review by the accreditation authority or identity provider, where disclosure is considered necessary, too. And then two cases fulfill and meet an applicable legal [inaudible]tion of the accreditation authority or identity provider or by carrying out an audit under this policy.

So this is the proposal for consideration of the team as seen now on the screen. With this, I would like to open the floor to see, first off, on C, whether that meets our joint understanding.

I see no requests. Then D.

Marc Anderson, please?

MARC ANDERSON: Thanks, Janis. I'm just raising my hand so you know we're listening. We think they're good. Thank you.

JANIS KARKLINS: Could you raise your hand more frequently with this message?

Dan?

DAN HALLORAN: Thank you. I'm not sure yet. I'm just a little concerned that it might be overpromising confidentiality, your secrecy, for all of the logged that data, that we could only disclose it in response to a legal requirement. There might be other cases where there might be something that was logged but we do need to disclose it for something. I don't know what yet, but in the ordinary course of running the system or to disclose it to the authorizer, maybe? I don't know. It'd hard to know. Like somebody else said earlier, without knowing how the whole system works, what we might need to do with that data … This is another one where it's a requirement that's not put in [inaudible]. It's not saying who must do what here. So it's not clear. It seems to be an obligation on the accreditation authority to keep that information secret. It's not clear to me yet if that's going to be realistic or possible.

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: Yes, Marika, please.

MARIKA KONINGS: Maybe a way to address this point would be, "Log data shall typically only be disclosed." That may give you a bit of maneuver.

[DAN HALLORAN]: Or something like, "Need not be disclosed, except for this." There might be other places that should be or has to be disclosed for some other good reason.

JANIS KARKLINS: I have Chris and then Alan. Chris, please?

CHRIS LEWIS-EVANS: Thanks. I'm just going to suggest maybe "meet contractual requirements" because that's what you're discussing there: the transfer between two bodies in a for[m of] contract. So just "meet contractual requirements" added to that list. And not [inaudible]. Sorry.

JANIS KARKLINS: So where would you suggest to put that?

MARIKA KONINGS: [It's a new C, or …]

CHRIS LEWIS-EVANS: C.

JANIS KARKLINS: Alan, please?

ALAN WWODS: Thank you. I agree with Chris. I'm thinking along the lines that contractual requirements meet even be slightly limiting, so something along the lines of "to support the reasonable functioning of the process (or procedure)" – I can't think of the right word there. But again, just to say that the ordinary course of business (the legitimate purpose, for want of a better term) is what we could put in there as well.

JANIS KARKLINS: Now that I think addresses also your concern then. This new C addresses your concern.

[CHRIS LEWIS-EVANS]: Yes.

JANIS KARKLINS: Okay. With this, can I take that as this is something we could live with?

Yes? Good. So it seems to be that we have finally had stabilized the building block on accreditation. I would like to congratulate all of us. It's not the end of the road. We will do the proofreading, of course, of all elements in conjunction with each other once the initial report will be

drafted. But at least I think we have made good progress on this. Actually, in half-a-day, we accomplished work which we would need probably about a month, if we count only the phone calls that we have weekly. So thank you for this.

So that would lead us to the next building block, which is acceptable use. If I may ask staff to put the text of the acceptable use building block on the screen.

Yes, Farzaneh?

FARZANEH BADII: Sorry. I'm late to the game. I think I'm not getting my [inaudible] properly. I think that the author – again, I'm talking about D and E about the logged data. I think, for the future, there has to be some kind of transparency report or some kind of requirement like that so that we can look at the functioning of these bodies and see how they have come up to the decision to disclose the data and be able to do this research in a way. I think that's maybe requiring them to have a transparency report. That'd be ideal. I don't know if we should go to the details of what the report should entail or anything like that, but I think at least they have to be transparent about how many requests they get or they disclosed the data and the transparency reports that Facebook and other social media platforms can put out there. Just flagging it. I don't know how to deal with it, but I thought maybe we can adopt something. Thanks.

JANIS KARKLINS: Thank you. We've just now finished the building block on accreditation. This is not touching the disclosing of personal data. So once we will get to the logging and auditing of the requests for disclosure, then we can talk about possible transparency reporting and [other] things.

Marika?

MARIKA KONINGS: I think that's a really good segue to remind everyone that those building blocks are up in Google Docs. We actually, I don't think, got any input on the logging and the auditing one. So, if you feel like doing something tonight, I would suggest you go and look at that. If you have specific language, even better. Or tomorrow morning, if [inaudible] wake up.

JANIS KARKLINS: Yes, but please do it before going to the bar. Or do it exclusively after, so then it will be very clear.

We have done a partial reading of this building block. First, let us look to the acceptable use policy on the requester's side. We have agreed on Sub-Point A and Sub-Point B. Sub-Point C was formulated by staff based on the conversation that we had.

Marika is correcting me. Please, your hand is up.

MARIKA KONINGS: Actually, I should take my hand down. I just wanted to correct that it actually was not staff who developed this language. I believe it was

Brian who put the new Bullet C in. I think Amr confirmed in his comment that he was happy with that added. So we applied it, basically.

JANIS KARKLINS: The question now is whether Bullet C may meet agreement of the team – at least preliminary agreement.

MARIKA KONINGS: If I can make one more point.

JANIS KARKLINS: Please.

MARIKA KONINGS: Thanks, Janis. Everyone thinks this should be wrapped together with D because we made updates as well in D, I think, to address some of the concerns that Amr expressed. I think that Margie had as well. So basically the proposal was to split it out in a new C and modify D accordingly.

JANIS KARKLINS: With that understanding, please read also D. "The requester must provide representation regarding the intent of use of the requested data. [For the] presentation, the requester will only process data for the stated purposes. These presentations will be subject to auditing." So Sub-Point C and Sub-Point D should be read in conjunction.

I have Hadia's hand up and then Brian. Hadia?

HADIA ELMINIAWI: I do agree with C. However, we have to keep in mind that, if the data subject asks for the reason for which his data or her data was disclosed, all the purposes will be mentioned in that case.

With regard to D, we say to only process the data for the stated purposes. I would say the stated purposes and other compatible purposes as well. A compatible purpose is a language coming actually from the GDPR. Thank you.

JANIS KARKLINS: Okay. I have already some reactions, but maybe I will take Margie and Alan before going to Brian in reaction to Hadia's comments.

MARGIE MILAM: Hadia, that was what we spent a long time in our little sub-group working on. I was with you on that in talking to Amr and others. That's how we end up with at least identifying multiple purpose. But I know he's not willing to support that.

JANIS KARKLINS: Alan, please?

ALAN WOODS: Thank you. What Margie said. I was party to one of those meetings and, yeah, that was where we ended.

JANIS KARKLINS: So there has been some work behind it. So I'm not saying to please take without consideration, but please be aware that there has been a lot of discussions already to formulate this by most interested parties.

Brian and Marc Anderson.

BRIAN: Thanks, Janis. I was of a similar mind as Hadia when we went into that call. What we did here was intended to address that. So hopefully, Hadia, you can meet us there.

I had my hand up to just note that we may want a little bullet or footnote here on the representation subjects auditing to just point over to the auditing building block so this isn't misconstrued to be talking about some different kind of auditing or anything that's not within the four corners of that audit building block. Thanks.

JANIS KARKLINS: Yeah. That's noted. That's understood. Marc, please?

MARC ANDERSON: Thanks, Janis. Could we get a quick second to caucus on these ones? Maybe just, like, two minutes?

JANIS KARKLINS: You can have three.

MARC ANDERSON: Thank you.

JANIS KARKLINS: So, Marc, what is the verdict?

MARC ANDERSON: Thanks, Janis. Hopefully I get this right. I think we would like to suggest updating D to read, "For each purpose … request …

UNIDENTIFIED MALE: For each purpose provided.

MARC ANDERSON: "For each purpose provided, must provide representation."

UNIDENTIFIED MALE: Yeah.

MARC ANDERSON: "For each purpose request," right?

ALAN WOODS: "Each purpose stated?"

UNIDENTIFIED MALE: Yeah.

ALAN WOODS: “For each stated purpose.”

UNIDENTIFIED MALE: Yeah, there we go.

ALAN WOODS: Sorry, Marika. You’re a saint.

UNIDENTIFIED SPEAKER: [inaudible]

ALAN WOODS: Yeah. “Must provide.”

JANIS KARKLINS: So now what you see on the screen correctly reflects your request?

MARC ANDERSON: Thank you. Yes, that covers it. With that modification, I think I can say we’re comfortable with it: C and D.

JANIS KARKLINS: So with the text which is now on the screen, C and D would be acceptable for contracted parties as now requested?

Milton, please?

MILTON MUELLER: I remember it was okay that a single requester could have multiple purposes. I don't know about this business of having multiple purposes per request. That strikes me as fishy in the sense that everybody is just going to list every possible purpose under the sun and hope one of them sticks. So, if they don't know what purpose they're asking for in the first place, why are they asking for this data?

So I look at the modification that was just made in D. Yeah, that's an improvement, but, if each stated purpose needs a different representation, why would they be the same request? I just don't get that.

JANIS KARKLINS: Margie, could you explain?

MARGIE MILAM: Yes. It's not meant to be that you drop down and pick any purpose just for the random thing. We were talking about the example where the request might have multiple purpose. A phishing event could be cybersecurity. It could also be trademark infringement. So you would put those down because you don't know at the onset which way you're going when you're asking for the data. After you do your investigation,

you might go the cybersecurity route. So that's what that was intended to address.

But the change that was made I think is confusing because, if you have one request and you're saying (just for the sake of argument) trademark infringement and cybersecurity, why would you also have to have two separate representations if it's meant … It just seems duplicative in how you would do it. So I need to understand it before I can comment further.

JANIS KARKLINS: Okay. James, can you explain now to Margie?

JAMES: I hope so, but I think the other contracted parties want to get on this. But I just want to point out – I don't know it says good thing about me or it says good things about Milton – that's pretty much word for word what I just said over here that I was concerned about. The reason I think this addition addresses it is because it essentially does not allow for any orphaned purposes so you cannot just shotgun a bunch of purposes along with a request and figure out which one sticks. Each one had to have all of the representations. I agree with Margie that, in the case where the purpose in a singular instance is clear, it will feel duplicative to do those, but what it does is it guards against those orphaned purposes, where someone is maybe "Here's three. Pick the one that passed the balance test." That's what I think we're trying to guard against.

So, while it does feel like extra busy work or copy-and-paste the representation three times, I think it prevents abuse of the – while still allowing multiple purposes to come through on a single request.

JANIS KARKLINS: Thank you for these explanations. I think they help us get closer to consensus or at least a common understanding.

Brian, please?

BRIAN: Sure. Thanks, Janis. I'm happy to answer Milton's question because we said the same thing. The concept was that what we wanted to avoid, along with Amr, was a situation where we requested WHOIS data and we said, "I'm going to mail a cease-and-desist letter to this bad guy," and then we do that and there's developments down the road and then we want to sue the bad guy. So we want to avoid the situation where, when we go to serve him with process, we don't have to go back to the SSAD and say, "Now I have a new purpose for this data, which I already have. I need to check that in with the SSAD and get permission to process the data for that purpose." In order to avoid that, we would say in the initial request, "I have a couple purposes here. I'll only use it for these purposes. These are the purposes," so that there's no going back into the SSAD to do that. So that's what this was intended to fix. So this was a solution to that problem, if that helps everybody get up to speed on where it came from. We had the same thought, too. We're happy with how it turned out here.

JANIS KARKLINS: Thank you. Mark Sv?

MARK SVANCAREK: I'm okay with the language as it is right now, but I thought we had been going down a slightly different path, which was, rather than having multiple purposes, we would just define our purposes more clearly and say, "My purpose is the investigation of a crime involving a domain name. Here's the three kinds of processing that will be associated with the purpose." So one purpose might have multiple processes, but it's still only one purpose. I thought the way we were going, but this language works for me, too.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. Just for clarity, if I make a request with two reasons and two rationales and one of them passes muster but the other one doesn't, does the information get released? Is it an either/or or a both?

JANIS KARKLINS: Alan Woods, please?

ALAN GREENBERG: Whatever the answer is, it should be made clear in the wording.

ALAN WOODS: My take on that would be, yes, if it's the same data set in both purposes, one would be realized. The other one wouldn't. You'd have the same data, but you yourself are required to only apply with that purpose that was given. So that makes sense.

On Mark's point, I actually think potentially that there's a good mix in the middle because, if a person who's requesting a disclosure is moved to put in that much detail and effort into it and there is a mix of purposes within that one request, then that doesn't necessarily mean that will not be approved either because you're giving that detail, you're giving that thought process, which is so vital to the disclosure process. So I think they're actually both the same. I'm good with it.

JANIS KARKLINS: Thank you. So, so far, I do not hear opposition.

Farzaneh, your hand was up. Not any longer. I'm not insisting, but just making sure.

FARZANE BADII: You are insisting. I'm just very uncomfortable with C because it's not really clear what it means. Does it mean that they may request data from the SSAD about one domain name with multiple purposes or various domain names with various purposes? It's just not clear and I'm not comfortable with it.

I think the thing that should be done here is to clarify what we mean by data and "for multiple purposes." I think we need to reflect upon that a little bit more. Thanks.

JANIS KARKLINS: Chris?

CHRIS LEWIS-EVANS: Thanks. Hopefully to help Farzaneh out a little bit, maybe if we add multiple compatible purposes in there because I think that's what we're trying to cover: you've got a domain name and you're going to carry out multiple actions on that domain name. So you have a number of different purposes for processing the data for that.

So what we want to allow is for that multiple processing to occur, but realistically, they've got to be compatible with each other. We don't want to release the data so you can block the domain because it's sending spam but then also sending [them] some marketing details. They're not two things that should ever go together. So maybe if we add multiple compatible purposes because that's what we're trying to do, isn't it: just have that process in for that breadth of activity that can be carried out. Thank you.

JANIS KARKLINS: I think this also needs to be looked at in the context of, overall, our discussion and how we're building the system. I think one of the first principles that we agreed on is that there will be unique requests of

disclosure, which means one request per domain. But that is overall overarching, so we need not to clarify every time that each request is unique. Here the question is, if, for the one domain name, there might be reason to ask questions for different purposes … That is where we are at.

I think we have reached common understanding. That's my feeling. But, Thomas, your hand is up. I hope that you are in agreement with me.

THOMAS RICKERT: I am. I'm just wondering whether we need this language because, if you are asking for disclosure based on a different legal basis potentially for a different subset of the registration data – Farzaneh, that's [bearing] on your point – I would treat that entirely separately. It's a separate case, basically, that you're making. I wouldn't know how we technically conflate different types of requests. Then everything falls into their places naturally. It may well be that one request is granted and the other is denied, depending on whether you fulfill the prerequisite requirement. But if you want to clarify, clarify away. But I think it's not needed.

MILTON MUELLER: When you say it's not needed, do you mean C or D or both?

THOMAS RICKERT: C, I mean.

MILTON MUELLER: I agree.

UNIDENTIFIED FEMALE: I agree.

UNIDENTIFIED MALE: I agree.

MILTON MUELLER: Because D implies there might be multiple purposes.

JANIS KARKLINS: Volker?

VOLKER GREIMANN: I get that, and I fully agree with what's stated. However, if it gives comfort to some members of the group to have that language in it, it wouldn't be hurtful to any of us. I think there's no harm in keeping it in. I don't mind it being in there. I agree that it serves no valid purpose, but it gives members of our community peace of mind, then why not?

MILTON MUELLER: It makes Farzi uncomfortable, and you don't want to make Farzi uncomfortable.

JANIS KARKLINS: But Farzi was uncomfortable for a different reason.

FARZANEH BADII: No.

JANIS KARKLINS: I explained that each request is unique.

THOMAS RICKERT: Sorry for jumping back in. If I had to implement this policy, I would see this as a requirement for me to build something that allows for one request to support different purposes and spell out different requirements. I think that's something that we technically don't necessarily won't do to. If you want to take Route A, let's say, that gives you access to the full set of registration data and then you have another purpose that might only give you access to a subset thereof, that would be different technical processes, different queries. But if you don't see an issue, I don't want to create one for you.

JANIS KARKLINS: I think we need to listen to each other. There was a very clear explanation for why this multiple-purpose request could be filed in the first place. If that does not create any difficulty but is seen as, let's say, useful for follow-up legal action that may be taken, why not?

Farzaneh?

FARZANEH BADII: The topic that Thomas is actually presenting here, which I agree with – and I tried to say it myself but I couldn't properly – is that the substance of the data also is important. So it's not only about the domain name, or if it's one domain but it's also the subset of data … We are very unclear about what we mean by data. In the implementation process, if we have multiple purposes for various subsets of data, that would be problematic. But, again, I'm not going to continue insisting. I'm just going to remain uncomfortable. I will take my revenge.

JANIS KARKLINS: Thank you. I have five hands up. If you don't want to speak, then please take them down. I have Alan Greenberg, Brian, Margie, and Stephanie, in that order.

ALAN GREENBERG: Thank you very much. I can certainly live with putting back in the word "incompatible" since that's where this came from before we had multiple. I could live with saying "only if they have the same data subset associated with them," because at this point we don't have an awful lot of redacted data. So we're not going to have that many variations.

However, I don't think it would be reasonable to say you have to submit multiple requests. If indeed these things are going to be handled in a completely automated way, it doesn't matter. If they're going to be handled in a manual way, they may end up going to the registrar and going to separate queues of separate people. If you have three compatible needs, they would be handled by three people

independently, tripling the amount of work, which I think is a ridiculous thing to do when we can handle them all at once. Thank you.

JANIS KARKLINS: Thank you. Brian?

BRIAN: Thanks, Janis. I'll take Milton's word of caution and try to make Farzi more comfortable with this. To do that, I would suggest maybe that we include some kind of linkage or some kind of perhaps thought here – or maybe we make the update in the other building block – where we talk about the query policy and we reference the purposes per requests over there. That might help because that's where we have the requirement about that you ask for the data elements that you need and you represent that those are the ones you need. That's somewhere else. So maybe Farzi's more comfortable if we make sure that that is contemplated there. Thanks.

JANIS KARKLINS: Thank you. I think we need to have a conceptual agreement. Then it doesn't matter where this conceptual agreement is reflected.

Margie?

MARGIE MILAM: I just want to emphasize that it is important for us to keep the multiple purposes as per the … Otherwise, we go to back to the point that Hadia raised.. I don't want to relitigate that, so let's keep it in.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Thanks. I regard C as necessary. I think that you have to have that clarification. I don't know where the compatible language came from, but purposes don't have to be compatible. But definitely you don't want to have to put in multiple requests for different purposes. That would be a nightmare. I don't even think that you need to parse out which data elements are for which data requests in the actual form in the RDAP. So I don't know. But I hope Farzi is feeling more comfortable by my assure that – trust me – C is needed. Thanks.

JANIS KARKLINS: There is a suggestion Alex made. Alex, could you outline what you're suggesting?

ALEX DEACON: I think it was just supporting what Brian said earlier. If it makes people happier to link it to data that was requested, then I think we'd be okay with that.

JANIS KARKLINS: But you have a very concrete proposal. Could you outline it?

ALEX DEACON: Well, I'm not too sure how concrete it is. It was just in the chat where I basically stated what I thought were the facts, which is that C allows for multiple purposes to be expressed per request. It sounds like we're all okay with that. Then (dot-dot-dot) for the same subset of data requested, how and where we express that in our policy and whether it's done in this building block or elsewhere. I didn't get that concrete, but I think, conceptually, that's what I had in mind.

JANIS KARKLINS: Now, that conceptual understanding is put in C. "May request data from SSAD for multiple purposes per request for the same subset of data requested." Yes?

UNIDENTIFIED FEMALE: I like it.

JANIS KARKLINS: If you like it, then everyone likes it. So, with this understanding, can we say that C and D are something we can live with?

Brian?

BRIAN: Thanks, Janis. The smallest nitpick ever, but can we say "set of data"? Because I don't want to assume that it would be a subset in every case.

JANIS KARKLINS: Yeah. Set of data. Whew! C and D? Done!

E?

Stephanie, I think your hand is old.

On E?

With that, I understand that F goes or there is something else for F.

Chris?

CHRIS LEWIS-EVANS: Thanks. The red language I don't know that we need, really. We've already said "in compliance with applicable law." So why are we then detailing what applicable law is? So I really don't see the need for that red language. Thanks.

JANIS KARKLINS: But I think we agreed to use, through the whole policy, this formulation: "in compliance with applicable law."

CHRIS LEWIS-EVANS: Yeah. So that's fine.

JANIS KARKLINS: Yeah.

CHRIS LEWIS-EVANS: So the applicable law bit is fine. It's the "including keeping a record of processing activity where required." I just don't think that bit is needed.

MARIKA KONINGS: Can I comment on that one?

JANIS KARKLINS: Yes, Marika.

MARIKA KONINGS: Thanks, Janis. I think that was added specifically in response to a comment from Hadia. So just looking at Hadia for if she's fine with taking that out. I think others have made the point as well. If you say "applicable law," you should already cover everything and you don't need to spell it out. But I think Hadia on one of the calls made this specific call, so if she's maybe happy with deleting it, it may be an easy one.

JANIS KARKLINS: Question. Would everyone be happy, or would it be acceptable, to delete "including keeping the records?"

HADIA ELMINIAWI: Yes, I agree with deleting it.

JANIS KARKLINS: Okay. So then we will keep it simple. So, with E, we would keep just "must handle data subject's personal data in compliance with applicable law." Full stop.

Dan?

DAN HALLORAN: To keep it even simpler, you could just get rid of it because everyone always says to follow applicable law anyway. There's no need to put it in individual policy requirements. You haven't put it on all the building blocks, that we have to follow applicable law. It's always assumed and implied. It's not really harmful, but it's not necessary either.

JANIS KARKLINS: Yeah. Okay. But since it's not harmful … Again, we may, when every block will be put in sequence, consider getting rid of similar sentences in every block, putting it in one statement above everyone and saying, "All these policies should be compatible with applicable law," full stop. Then we get rid of every other thing. But let us keep it if that is not harmful.

Alan, please.

ALAN WOODS: Just to play devil's advocate for a second – I'm not saying I support this or not – one of the things that makes sense and may help whoever the

SSAD is – because it's the link to the auditing building blocks, specifically here – having a record of processing as a requirement of the SSAD, saying, "You must keep a record of processing of this," could be advantageous and helpful in an auditing process. But I'm not married to that. I just think, yes, it is required under law, but if it is required specifically and ultimately reminded for people who apply to that … But, again, I'm just trying to play devil's advocate and maybe port it in there.

JANIS KARKLINS: Okay. How about the proverb that the better is the enemy of the best? Again, this is not the end of the world. It's not the end of the reading. We are just stabilizing. Then we will do the final reading of the whole document, looking for incompatibilities and things that need to be fixed. We will take it from there.

With this, we also stabilize E and we delete F, since that says nothing. We move to the next – yes, please, Farzaneh? Oh, yeah, your hand is up. Yeah, please.

FARZANEH BADII: I'm sorry. Yes. I just wanted to ask a clarifying question. When we say that the data subject's personal data should be treated responsibly or in accordance with the applicable law, doe that mean that, if the requester resides in a country where there's no privacy law, they can just publish it somewhere on the net and benefit from it. This wording "as applicable law" I think is very … because we are giving global

access, I believe. We are globally disclosing this data, and conditioning the safeguarding of this data by the requester upon the applicable law might not provide a lot of protection for the domain name registrant.

So this is just something that I want to flag. I have seen this throughout, that we talk about applicable law and data should be protected according to applicable law. But what if there is no applicable law? And we should consider that we are providing global access. We should have global data protection, too. Thanks.

JANIS KARKLINS: I think that the reason why we're using applicable law is to make sure that this policy could be enforced or applied, not only for GDPR but for any other future data protection laws that will be adopted somewhere.

So, from the other side, ICANN is not a lawmaker. ICANN only follows laws and implements them, not puts them. If there are territories or states where private data is not protected, then probably ICANN should follow the applicable data of that particular country. Otherwise, there might be other consequences. Again, we're looking from a different side.

So, today, private data is not protected at all and is available to everyone. We're addressing issues when data is protected by law. More and more this private data will be protected by the law.

Margie?

MARGIE MILAM: I think this is a little problematic if you think about, for example, cases where you're using the data for a lawsuit. If you're suing someone, that becomes public record – their name. That becomes part of the legal process. So we just want to make sure that we're not putting in roadblocks for things that are allowed under law. So that's an area where I think this language is problematic because it goes beyond what the potential legal requirements are and we're not thinking through all the different scenarios.

JANIS KARKLINS: Which language are you referring to, please?

MARGIE MILAM: J.

JANIS KARKLINS: You're ahead of me.

MARGIE MILAM: Oh, okay.

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: Let me get, since I cannot see that on the screen … So, Building Block H. We're now talking about the entity disclosing data. We have done

some discussions on this one already. Now we are on H. H? Yes, H. Margie was uncomfortable with H.

MARIKA KONINGS: She was talking about J, not H.

JANIS KARKLINS: Oh, okay. So let's take them one by one. On H, you're not the first one. Alan Greenberg, please. On H.

ALAN GREENBERG: Well, I actually had my hand up for the previous one.

JANIS KARKLINS: Which previous one?

ALAN GREENBERG: In response to Farzaneh's comment.

JANIS KARKLINS: Oh, okay. Please, go ahead then.

ALAN GREENBERG: The law applicable where the data recipient resides is not really the issue. If you get data from the SSAD, you are agreeing to how you're going to use it.

Now, that may not the law of your land, but you're essentially signing a legal agreement on how to use it. Now, you may not be prosecutable if you're in a country where I can't reach you, but, nevertheless, the data has been protected recently because the recipient has agreed to abide by the law of the land, essentially, where the data releaser was. So, it's a personal contract, not necessarily enforceable, but it's not the law where the data receiver resides that is really the one that's, in theory, governing this. So this is as good as we can do.

JANIS KARKLINS: Volker, on the same?

VOLKER GREIMANN: I agree but disagree with Alan. Having a simple agreement in place is not sufficient under the GDPR. There must be an element of enforceability. If you're not able to enforce that agreement and you willingly sign an agreement that's not enforceable, then you will still be liable for that violation if a violation happens by that party that you then cannot enforce against. So there is an element there that we should have that enforceability as well. So just to qualify that.

ALAN GREENBERG: Let's hope there's extradition laws for data privacy violations then.

JANIS KARKLINS: Can we move back to the text and focus on formulations in Building Block H? We are now on Sub-Point H in Building Block H. Who wants to speak on that?

Brian?

BRIAN: Thanks, Janis. I was hoping we could get to this. While I agree with the first sentence in H, it needs to get out of here and we should definitely do that and we should do that well. But I don't think that pertains to the entity disclosing the data. It looks like it pertains to the contracted party who's collecting the data in the first instance. Then I think the rest of what I see on the screen there under H is probably pretty good. Thanks.

JANIS KARKLINS: So your proposal is to take the first sentence out and put it an obligation of the contracted party, probably at the moment of collecting data?

Okay. Noted. Milton?

MILTON MUELLER: I'm sorry about this, but I wanted to address the comments about logging that are in the staff support team comment. When would we do that?

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: When we will be talking about the logging building block.

MILTON MUELLER: Oh, there's a separate building block?

JANIS KARKLINS: On logging, yes.

MILTON MUELLER: Okay.

UNIDENTIFIED FEMALE: [inaudible] tonight.

MILTON MUELLER: Sometime later tonight. I'll assumedly still be alive by then.

JANIS KARKLINS: Matt?

MATT: Thanks, Janis. Brian started to pick up on what I was going to flag on H in that the disclosure is going to happen to the data subject via the registrar. But then, when the data subject wants to understand the processing activities of their data within the SSAD, they'll then go directly to the SSAD operator. I don't have a solution for that, but I just

want to flag that as something we're going to have to think about a little bit more because there's going to be a big disconnect there between the data subject thinking that they've provided this data to the registrar, and then there's this third-party entity that actually is going to be the party disclosing it. Thanks.

JANIS KARKLINS: What would be your fix for that?

MATT: I admittedly don't have one right now. Maybe that's more of an implementation issue. I don't know. But I wanted to flag that as something that we need to think about a little bit more that I don't think we can necessarily resolve here.

JANIS KARKLINS: Specifically, we are now taking out the first sentence and we would put it under obligation of contracted parties. But then the second sentence – "Upon the request of the data subject, the exact processing activities of their data within SSAD should be disclosed as soon as feasible." Would that be okay as a formulation, Matt?

MATT: That's definitely better, for sure.

JANIS KARKLINS: So yes?

MATT: Yeah.

JANIS KARKLINS: Okay. Milton, your hand is still –oh. Milton has disappeared. Okay. Brian, your hand is up? Or – yeah. Please.

BRIAN: I'm going to propose a fix. That language, as Alex mentioned in the chat, should probably scoot over to Building Block M with some specificity here. I think we all know what we've needed to do for some time is beef up 3.7.7.4 in the RAA. That 3.7.7.4 is what the registrar needs to tell the registered name holder at the time the data is collected. So we need specificity about the purposes. That's where that sentence that should go, I think, as a policy recommendation that says, "The RAA should be amended 3.7.7.4 to inform the data subject about that," and also about how they go to the SSAD to get information about how their data is being processed and perhaps what the registrar needs to do or how the registrar needs to refer the registrant to the SSAD if the registrar receives a request from the data subject about how their data is being processed. There's those three or four things that need to go with that sentence over to M and become a policy recommendation to update 3.7.7.4. Thanks.

JANIS KARKLINS: Okay. Could you send what you said to Marika and Caitlin? Then they can exactly know what you're suggesting.

With that understanding, I take it that we may delete the first sentence here and agree on the second? No, we can't.

Dan, you're first, then Chris and then Georgios.

DAN HALLORAN: Thank you, Janis. I'm concerned about the second sentence of H. I thinking about the hypothetical where we don't know what "entity disclosing the data" means yet. If ICANN is operating a central gateway and if it works according to the way the TSG prescribed it, ICANN would get the data from the registrar, parse it, send it to the requester, and then delete it. So the central gateway would not know anything about user data the second the request was handled. So, if a user came along and said, "Please tell me how my data was processed," the gateway would have to say, "We don't know. We don't know anything about you." Here it's saying the entity has to tell the user, the data subject, what processing activity was done. Thanks.

JANIS KARKLINS: Thank you for raising this issue. Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. I think we need to leave this in here. The reason is that – this goes to Matt's question – you have the contracted parties that get told they need to release the data but they don't necessarily have …

Let's just say we have a system where they don't make that decision. They're telling the data subjects what processing activity their response is going to be. We will release data to the SSAD, and then the SSAD will have to properly inform the data subjects who is processing their data. Therefore, that first sentence covers that instance where the contracted parties say, "Your data is being processed by the SSAD." There could be an explanation of what that is. But then what type of third parties would have to be detailed by the SSAD? So that's my thoughts on why we should maybe leave that first sentence in there.

Looking at Matt's face, I might not have explained that clearly.

JANIS KARKLINS: I don't have any hands up except Brian. Is that a new hand or an old hand?

Honestly, I'm not sure where are we. Can somebody talk to Dan's concern about if that is a centralized system and a central gateway that's just passing on information? Who will be informing and how the data subject … in case the data subject is asking a question?

Georgios?

GEORGIOS TSELENTIS: I just wanted to add to what Chris just explained. The way we have the second sentence is that we are talking about processing activities, which not necessarily are in the knowledge of the contracted parties, which was the initial concern of Matt.

So, if we want to keep the second sentence – "The data subjects want to know the exact processing activities about their data" – we need to add there what Chris said, that this type of information should be provided by the SSAD, by whoever is the operator of the SSAD, because they have the knowledge, not necessarily the contracted parties.

So I don't have a complete sentence to that, but I think we need to keep the second part of the paragraph and we need to add that "provided by the operator of the SSAD." So this type of information about the processing activities needs to be given by the operator of the SSAD.

JANIS KARKLINS: Thank you. Alex?

ALEX DEACON: I think, in terms of Daniel's question, even if the centralized gateway operated by ICANN – the decider, if you will – deletes the user data, there's still going to be an indication, a log, that a request came in, that it was processed. There may be certain logs where states of the request have changed. Eventually there'll be a log entry that indicates what the response was. So, whether that's exact processing activities for their data, I don't know whether that meets those words. But I think there's enough information in those logs to indicate to the data subject what happened to their data and when.

JANIS KARKLINS: Thank you. Let me take a few others and then come back to you. Alan Greenberg, Mark Sv, and then Dan.

ALAN GREENBERG: Thank you. This is more of a question than a comment. If logs are being kept and we know data can only be kept as long as it is needed, what are the requirements for how long to keep logs to answer requests from the data subjects? Is there a period for which you must be able to respond and, after that, you can delete you logs? I don't recall talking or reading about that before.

JANIS KARKLINS: I think we have not really talked about the logging building block yet.

Mark Sv, please?

MARK SVANCAREK: I do have a concern about this. If I were the data subject and I went to my registrar and said, "Please disclose the processing that's happened to my data," the registrar would say, "Remember that central decider that I told you about at the moment of collection? I have (or have not) transmitted your data to that central authority." That's what you could say.

If they went to the SSAD operator and said, "Have you processed my data?" the SSAD operator would go the logs and say, "Which data is yours? Because I don't know that the data subject's identifier was necessarily sent along with their registration data." We just need to

figure out how they identify within this system. How do you map it to the logs? Do you have to produce the RDS record itself and say, "I am __. Registrar =this string. E-mail address = this string. Please show me how my data was processed"? It seems like you could implement it that way, but I just want to make sure that we think about that detail right now so that we don't get down into the implementation and discover that we've left ourselves a hole.

Hopefully that makes sense. Depending on how you ask, it might be easy to verify which processing happened. It might be harder. How do you demonstrate that you are the data subject? What identifiers do you need to provide in order to get the information back? If I registered something as mark@microsoft.com, but the registrant in the RDS is domainoperator@microsoft.com, how do I demonstrate that I am that same person? That's my consideration. So maybe we should talk about that.

JANIS KARKLINS: This is what we're doing. Daniel?

DAN HALLORAN: Thank you. I think Mark Sv is hitting on it. We almost half to build a reverse SSAD, where a data subject can go to the registrar and say, "Hey, I want to know who got my data." The registrar would say, "I responded to the following ticket numbers with a copy of your data to the SSAD." Then somehow you'd have to be able to pull from the SSAD who got the data on these tickets and then feed that back. If you want

to build that, it would have to be a reverse-passthrough SSAD to send that information back to the registrar or back to the data subject. But just Mark Sv cannot come to the central gateway and say, "Hi, I'm Mark Sv. Please tell me when my data was processed," because the central gateway would not know.

JANIS KARKLINS: But isn't that link put in the domain name? That domain name will be logged anyway. This is not public, personal data. It's a domain name. If every individual who will be asking about his or her data will be referring to his or her domain name, that will certainly be kept in logging information.

Yeah, please.

DAN HALLORAN: That's possible. I haven't thought through the detail of what has to be logged and what has to be deleted. Just a little bit of caution, though, that we can't necessarily say that domain names are not personal information. So that's just to put a wrinkle and complicate things. In some cases, they can be. They can be identifiers. They can include personal information. So we can't dismiss that out of hand.

JANIS KARKLINS: If Mark Sv registers a domain name, marksv@me.com, then that is his choice that he – sorry that I'm picking on you. So it was purposely put. I know many people who purposely put in the domain name indication

that that is a specific individual behind it. So that was a choice, so we cannot do anything about it. But, again, I'm not really an expert in that.

I have a huge line now. I have Volker, Brian, Alan Greenberg, and Mark Sv in line.

VOLKER GREIMANN: I'm a bit worried at the moment because I have a feeling that we're creating a monstrosity that not even a mother could love. I have been thinking about this and I was thinking that maybe we could channel the requests through the registrar and basically they would get a button in their interface that would lead them through the SSAD and have them pre-authenticated by the registrar when they log into the SSAD through that functionality. But even then you have the issue that, in many cases, the account holder is not actually the registrant or the data subject. We have many cases where account holders register domain names for many different people. So that's not a solution, either.

So how do we identify the data subject? We have issues where we are quarreling with domain owners that are refusing to identify themselves. They may have control of the e-mail address of the domain holder but they are not providing any further documentation. So we usually err on the side of caution when we they make certain requests for modifications on the domain name.

This would be the same situation. Somebody is coming to us, saying, "Hey, I'm this-and-that person. I really am but I'm not going to prove it to you." Where do we go with this? I think we have a very, very difficult

problem identifying people, especially when data protection laws and additional legislations also limit the methods that we can use to identify a person.

For example, in Germany, we're not allowed to ask for a copy of the national ID card because that contains information that only the ownership know. We are not allowed to ask for a copy of the ID. How do we go about identifying that person? We need to find supplemental ID. It gets complicated the more jurisdictions you enter.

So this is going to be a complicated issue. I think probably a lot more thought needs to go into this.

JANIS KARKLINS: Okay. Let's gather the thoughts of others. Brian?

BRIAN: Thanks, Janis. I think I'm up to speed on this conversation. I was working on try to fix this problem [in] my note to Marika and Caitlin here. I think what we need to do is what the law requires, as far as the data subject exercising their rights. I think we'd be willing to accept a bit more so that this whole thing works well. So the data subject has the right to obtain, from the control, confirmation about whether the data is processed and, if it is, more details than that. The system that we seem to be working on, the SSAD or probably ICANN as what we're aiming for, will be the control. Then, from a common sense standpoint, I think the registrant probably only know who the registrar is. When we

beef up 3.7.7.4, they'll in theory at least know a little bit more about who to contact to ask for this data.

So I think a policy recommendation that requires the SSAD to provide those logs to the data subject would be good. The SSAD is going to have to figure out how to do that. I don't know if we need to solve all the world's problems and tell the SSAD how to validate that that person is who they say they are. There's probably services or technologies or expertise that will come over time that will allow the SSAD to identify who that person and make sure that they are who they say they are before they cough up those laws. So we should recommend that they do that and then have a real rough draft policy recommendation for the registrar to also instruct the data subject on how to go to the SSAD and get those logs about that from the SSAD, too.

So I'll send those to Caitlin and Marika and maybe they can much them much better than they are now and we can take a look at them together soon. Thanks.

JANIS KARKLINS: Thanks, Brian. Alan Greenberg and Mark Sv.

ALAN GREENBERG: Thank you. I facetiously sent a note to Mark saying, "It's simple. The SSAD has to make an SSAD request to find out who the owner is." But the reality is, I think, that a request for at least logs is going to have come through the registrar, and the registrar will request it from the SSAD and pass it back. Or the registrar is going to have to provide some

sort of token of validity to the registrant to present to the SSAD because the SSASD is not going to have any information that links it to an entity who has the right to request the data that it can guarantee.

So it's going to have to be done in conjunction with the registrar with the data flowing in one direction or another. I don't see any other way out.

JANIS KARKLINS: Thank you, Alan. Mark Sv?

MARK SVANCAREK: It does seem like it'd be easier to implement if the requests all go to the registrar and the registrar can interrogate the SSAD for what processing has happened. Volker did raise an interesting question, where the account holder is different from the registered name holder. I guess we can figure that out, but it does seem like a tricky additional wrinkle. I would very much like to solve this problem so that a data subject can request directly to the SSAD operator and just have them come up with an actual implementation that, I think, works.

So, until then, I think we have to consider that our policy will be that the data subject must ask the registrar what processing has occurred. I don't know what the level of the obligation is under the law. If I say to the registrar, "What processing occurred?" and you say, "Well, I provided your data to the central authority, that one I told you about," is that sufficient? Or do you have to say, "All the processing happened once that central authority became a new data controller"? I'm not sure

that's actually a legal obligation, but, I don't know, we should think about that.

JANIS KARKLINS: Okay. Alex, your hand is up? Or is that an old hand?

It's an old one. So then I have Alan Woods and Milton.

ALAN WOODS: Thank you. I may try and be a bit pragmatic here. A lot of this discussion really does base itself on what the SSAD actually would look like. I think we're probably going to keep going around in circles and putting new layers on this. Until we know what the actual SSAD is, it's very hard to define his. So I potentially would suggest to the team that we're going to have to put a pin in this one and move on for expediency purposes because we're not going to get this today. When we define it more, we will. But, at the moment, I think we probably are beating a dead horse at this particular moment in time.

JANIS KARKLINS: Okay. If you say so. Milton?

MILTON MUELLER: I would kind of second that. I think the discussion I hear about a registrant gaining access to what data of theirs that was processed sounds like the concerns that I have, which I was told were part of the logging building block. I think, when we talk about log and who gets

access to those logs, that's where I thought that discussion was going to be, not in this particular building block.

Then there's a question of who makes the disclosure, which is still unresolved, at least in my mind. Some of the people talking about this sound to me as if they're assuming that the disclosure decision will be made by whoever runs the SSAD that is a single, centralized point and not by the registrar. But if indeed the registrars are the ones making it, which is probably the outcome I prefer, then they would certainly have a record of what they did and we wouldn't be assuming that they would have to go to the SSAD and ask, "What data did I disclose?"

So I think we really do need to know a bit more about how this system works before we can resolve these questions.

JANIS KARKLINS: Thank you, Milton. Then I would suggest that we keep H in square brackets until we will know more of how the system functions.

Let us then move to the next sub-point, which is J. So who would like to speak on this?

Chris?

CHRIS LEWIS-EVANS: Sorry to pull you back to the previous one. I know, when myself and James submitted this, we'd actually talked about having this as two separate points. So where it starts "However" should be a separate item. And this should not be treated one concurrent point.

JANIS KARKLINS: Okay. Let me then see the part from "However" on the screen now. "However, the nature of the legal investigation procedure may require SSAD and/or the disclosing entity to keep the nature of existence of these requests confidential," and so on.

Can we agree on that language, or we need to keep it as well in brackets until we know how the SSAD will function?

Any reaction? I think there's nervous giggling in some corners.

Alan?

ALAN WOODS: Thank you. I've read that a few times now again and the one thing that seems to be missing in my mind is, who decides whether or not it should be withheld from the data subject? This is just a key thing. In my mind, it would only be where a legal obligation or something exists, and I don't think that comes across fully in that. So maybe we can insert that somewhere, some consideration where it must be a legally based prohibition on release.

No? Okay.

JANIS KARKLINS: Chris?

CHRIS LEWIS-EVANS: We have a long discussion on this with James. What turned out to be a webinar was supposed to be small group, but I think it was quite well-attended. Really, the second sentence I think goes to that point, where all we're asking for is, when you do get a request as a contracted party, you say, "We've had a request. Can we release this?" and then that conversation starts. That already works in a number of cases. We have numerous other systems whereby that works. If you say, on the balance of this, to them, "We have to disclose," that's fine. All we're asking for is that conversation. We agree data [is] disclosed. Most law enforcement agencies have processes where they have to disclose data. So we're not saying you can't. This is a "If we've marked it, can we start a conversation?" If you're going to tell us you need to release it for legal reasons, then that's fine. But it's just having that conversation [for] putting that process in place.

JANIS KARKLINS: With these explanations, can we say that, [provisionally], this second part of the sentence could stabilized, starting with "However"? We would create a new sub-point starting with "However," which is now marked in red on the screen.

Matthew?

MATTHEW: We were just chatting about this over here, Chris. I think this may unfortunately also fall into the bucket of "We need to wait until we know what the system is going to look like," because, for example,

under the proposal from the Strawberry Team, we would completely blind as contracted parties to who that data is being disclosed to. So it would be difficult for us to say, when we receive a data access request from someone, "This has been flagged to law enforcement, so we need to consult with you and figure out a way to do that." So I think unfortunately this might be another one that we may have to work out once we understand the way the system is going to work.

JANIS KARKLINS: Thank you. Chris?

CHRIS LEWIS-EVANS: Thanks. In that instance, though, you would just know that the disclosing entity had released it. So you wouldn't know that it was law enforcement. So that responsibility not to pass … Now I can see where you're coming from. Yeah, I think that makes [sense].

JANIS KARKLINS: I think we need to park this issue until further notice. Volker you are not the only one in line, so I would say let's move and see how we can treat J. Then we will come to this point once we will see the outline of how the system functions.

On J, any comments?

I have two requests. Brian first, then Hadia.

BRIAN: Thanks, Janis. What is happening in J? I could just leave it at that, I guess. I don't like starting with "Must not disclose non-public data of legal persons" as a general concept, but then I think we really need to flesh out what these scenarios might look like, where the data subject – there's stuff with the strikethrough, too – is protected under … I guess it would be good to know how that would come into play. When would a legal person's data be protected under applicable data protection [inaudible]. I guess we could start with [inaudible] answer. Thanks.

MARIKA KONINGS: Thanks, Janis. This is one I think that went to a couple of iterations because I think it started out by talking about that we're not prohibited by applicable law. I think it was actually Volker who then suggested that maybe this should be done then other way around. I think most of these edits came from a call – I'm looking at Caitlin as well – where I think Volker made some suggestions on what that could look like. I think that got further modified after that language was reviewed again. So it went through a couple of iterations. As I said, originally it headed the other way around. I think then some suggested, "Let's look at it from the other side." I think that's how this ended up as it is now.

JANIS KARKLINS: Margie?

MARGIE MILAM: I think I'm confused by this section as well. Data subject? Are we talking about data subject or a natural person? Because it seems to me that

this prohibition shouldn't apply to a legal person if it's not a natural person. I think we just got to be more specific on what exactly we're talking about because it just seems too broad as written.

JANIS KARKLINS: Brian, your hand is up again.

BRIAN: Thanks, Janis. I'll yield for maybe more perspective on what we're trying to do here when I'm finished. Until we hear otherwise, I would really strongly need us to flip that back to "must disclose if it's a legal person unless something else happens." That needs to be the default. If the registrant is a legal entity, you have to provide that data because there's not a reason not to. You really don't want to get in between somebody who needs the data and a legal person that has no rights to not have this data disclosed. Thanks.

JANIS KARKLINS: Okay. Let me take Volker first and then I have Alan Greenberg and Chris.

VOLKER GREIMANN: To Margie's comment, I think "data subject" is the correct term if you're looking at this in the context of the GDPR, at least, because it's a technical legal term that's defined to an individual person who can identified directly or indirectly via the identifier such as the name, ID number, locations, data, and so on and so on. So it is by definition already referring to a natural person, not to a legal entity.

However, that might change if other jurisdictions and data privacy laws come into play. But if we take this term in the context of the GDPR, it's perfectly specific to natural persons.

JANIS KARKLINS: Alan Greenberg, please?

ALAN GREENBERG: Thank you. I was one of the ones confused by the triple or quadruple negatives in the original one. When I read this again, what I presumed it meant is, if there is information about a natural person in the registration record of a legal registrant – that comes back to a question I raised earlier today of whose responsibility is it if that's the case? Is the registrant who takes responsibility for releasing the information or the registrar?

The other possible implication here is that, in some jurisdictions, there are legal entities that are protected, be they charitable organizations or sensitive organizations in some ways. Maybe it's referring to that. I guess I'd really like to go back and try to find out what problem this was trying to solve. I don't remember anymore, but we seem to have someone over there who does.

CAITLIN TUBERGEN: Janis, this is Caitlin Tubergen.

JANIS KARKLINS: Yes, Caitlin? Please.

CAITLIN TUBERGEN: I believe this was something that Stephanie had raised about that there may be certain legal, as Alan noted, persons that are protected under certain data protection regimes. She gave a couple of examples, but that's why the language here is a bit broad.

JANIS KARKLINS: I would say we have … wait. Just a second. I think we have worked now for one-and-a-half hours, and I would suggest that maybe we need to have a little bit of a break, some 10 to 15 minutes. This is what I'm proposing now. We're scheduled to until 6:30. We can go on probably until 7:30 if needed. I'm joking. I suggest a ten-minute break just to stretch legs. Then please come back at 5:10 and we will continue this conversation.

In the meantime, please feel free to talk to each other on this topic.

UNIDENTFIED MALE: Can we send Milton on a beer run?

JANIS KARKLINS: So break until 5:10.

Okay, shall we start? Or shall we restart?

UNIDENTIFIED FEMALE: What if we say no?

JANIS KARKLINS: May I ask team members to take their seats at the table?

Hello? May I ask everyone to come to the table?

I think we can start recording. Thank you. We left the discussion of J. I think maybe we need to remind ourselves why we have this point and then see how far we can get.

During the previous discussions, we discussed that data subjects should have also protection in some specific cases. This is one of those cases. When a legal entity registers a domain name, that registration may contain also the private data of individuals. In some circumstances, this private data of individuals may need to have a special protection. That is why we are saying that this non-public data of legal entities should not be disclosed in certain circumstances. Those certain circumstances are if the data subject is protected under applicable data protection regimes or if the release of non-public data could cause harm to the data subject. These are specific circumstances of when this should not be done.

So that is the general context. We're trying to find an appropriate formulation of how that could sound as a policy recommendation.

I have a number of hands up, and I'm not sure whether that is the right order. Alan, Chris, Volker, Stephanie, Hadia, and Brian, in that order.

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: Okay. So let me propose the following. Please lower all hands and look at the text which is now on the screen, which is worked out by a group of individuals during lunchtime, which suggests that, in circumstances where the data subject is or its data is clearly identified as protected under an applicable data protection regime, such as special category data under GDPR, as the disclosure of this type of data could create more significant risk to a person's fundamental rights and freedoms. Extra safeguards must be implemented such as satisfying specific conditions under Article 9 [inaudible] data must not be disclosed.

I understand that the proponent of this formulation is Chris. Is that right, Chris?

So could you maybe speak a little bit about this proposal?

CHRIS LEWIS-EVANS: This is very, very rough and very, very quick. My recollection of J was it was trying to protect that the special category data that I think Stephanie highlighted in one of the calls. Under GDPR, it doesn't say that you can't disclose that data, but there are extra safeguards needed to be able to disclose that data under GDPR. Obviously, we're trying not to be GDPR-concentrated, but GDPR is probably the highest bar that we've got for this sort of data at the moment.

Like I said, it's very rough of what the disclosing entity or the contracted parties need to do, and it's really raising that balancing test up several notches. Extra safeguards are applied before a decision is made to release that data. So it's just trying to capture all of it. Like I say, it's very rough. I welcome any input, really.

JANIS KARKLINS: Thank you. Alan Greenberg, followed by Margie and Marc Anderson.

ALAN GREENBERG: Thank you very much. We're charged with developing policy that is implementable. I have a hard time understanding how one could possibly do this unless we come up with new data fields that flag various classes of special registrants whose data has to be handled differently. Even for that I'm not sure how we could implement it or how we can implement it in a timely fashion. So, although understand the legal requirement and I understand the emotional requirement that we should do it, how we could do it I find rather mind-boggling in any practical world that we're looking at.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I'm not opposed to the concept, but I still think this is too broad because, if you look at a data subject that is protected under an applicable data protection regime, that's all personal data. But we're

talking about a specific category. So I think we need to be a little more specific so that we clearly identify what we're talking about. Thank you.

JANIS KARKLINS: Thank you. Marc Anderson?

MAR ANDERSON: Thanks, Janis. I think Chris's revisions are good. I'm sure we can all get behind the principle that we're trying to accomplish here. This language seems principle-based, so I've no further revisions. I think what you did is good, Chris. Thank you.

JANIS KARKLINS: At the moment, I do not have any further requests. So what I would – Brian and … okay. Brian then Laureen and then Stephanie.

BRIAN: Thanks, Janis. I think we might not need to do this. If we're talking about Article 9 and that's where this is coming from, that's data about racial or ethnic origin, political, religious, philosophical – those kinds of things. That data is not in the registration data. Now, if that's on the website or in content, that's a different thing, but that's not the kind of data that we're talking about here. So I don't think we need to make an exception for this. Thanks.

JANIS KARKLINS: Thank you. Laureen?

LAUREEN KAPIN: Following on Alan's wise observation of what would be implementable, I'm wondering if somehow these inapplicable situations would really get factored into how the SSAD does the balancing test in determining whether the information should get released or not. Now, I don't know how the SSAD gets that information either, but Alan is right: these fields aren't collected. So, unless it's on its space by the name, I'm not sure how this percolates up. But if it does percolate up, then it seems to me it forms part of the balancing test.

JANIS KARKLINS: Thank you, Laureen. Stephanie?

STEPHANIE PERRIN: Thanks. I do apologize for putting this concept out and resulting in all those negatives. It was very confusing. It confused even me and I'm the one that proposed it.

I did come up with some draft language. In response to Alan's concern about how this is unimplementable, I'm reminded of the U.S. Supreme Court judge who was ruling on obscenity, I believe. He said, "I don't know how to define it, but I know it when I see it." I think that most registrars would know if it they see if they get a request to disclose, for instance, "Free Hong Kong Forever" as a domain name. They might think that, when the Chinese government came after them, there might be some human rights implications.

So here's my proposed language for that aspect of it. For the protection of people who are exercising free speech and human rights, when considering the publication – bear in mind, I'm not a lawyer, as I always say – of non-public data of legal persons, particularly with respect for NGOs and parties engaged with human rights activities that may be protected by local law – e.g., constitutional and charter rights law (or whatever language lawyers may prefer to describe that as) – data controllers/processors must consider the impact on identifiable individuals.

JANIS KARKLINS: Okay. Could you submit that language?

STEPHANIE PERRIN: I'll just snip and send it. Okay?

JANIS KARKLINS: Yes, please. That would be very helpful. So that would appear on this Google Doc. Most likely we will not close this chapter today, but that will stay on and allow us to reflect further on implementability of that request, whether directly or as a part of the balancing test.

Again, I have a few further requests for the floor. Daniel, Mark Sv, Marc Anderson, Volker, Alan, Alan Woods, and Brian.

DAN HALLORAN: The conversation should keep going, but I'm still very confused about J. And the text under J – I don't see how it relates to J. I understand the concept about the special categories. I think that's probably a topic the team could look at more and might even be subject for Byrd & Byrd – a question to them – but I don't know why we would limit it to just non-public data of legal persons. I thought it would be an issue for other data subject, too, like individuals who register domain names. If that applies, it would apply to them, too. I just have language trouble trying to understand, I think, like the early interveners, on what we're trying to say here. The first sentence in the new text under J seems like a fragment. Anyway, I'm confused by the whole thing and wanted to flag it. I don't know. We wouldn't know how to implement it.

JANIS KARKLINS: This new language is far from perfect. It's just a rough proposal. Stephanie will send in her proposal that we will clip in.

Again, I think I will take those requests that are still standing – Mark Sv, Marc Anderson, Volker, and Brian – and then probably we need to leave this conversation there and then move on and revisit it at a later stage when we have a slightly clearer mind after many hours of work.

Marc Anderson – no. Volker?

UNIDENTIFIED MALE: Well, I put my hand down in anticipation of going, but was I before Volker or was I …

UNIDENTIFIED MALE: [No].

UNIDENTIFIED MALE: Okay. I'll put my hand back up then. Sorry.

JANIS KARKLINS: There are too many mics open now.

VOLKER GREIMANN: Just to maybe clear up some confusion, Stephanie is right on the money. I think we do not keep that kind of data, but the nature of the domain name or the website published under the domain name might turn that data into such data. For example, if there is an atheist website that's based in Saudi Arabia, then providing the name and the address data of the registrant very much has to be seen in the context of that domain name or the content that's published thereunder. Therefore, it moves into the other category, whereas, with just a domain name that is known by them obviously in that is more specifically in that subject of that protected data but public at that time. The data can switch categories depending on the context. Therefore, providing that information in that context can turn into protected information as well. I think that's the main concern that J is trying to address and that we are trying to cover here. Hope that helps.

JANIS KARKLINS: I would like now to draw attention to alternative text that Stephanie has proposed. So please consider that. Again, we're not trying to close it today, just for the reference.

Mark Sv followed by Brian and then Alan Greenberg.

MARK SVANCAREK: Well, now we have new text to consider. My comment was about the phrase "clearly identifiable." It's the key phrase in the previous language, but also, how clearly identifiable is the concept of being clearly identifiable? I know it when I see it? I don't know, but it doesn't seem like great policy. But now that we have this new language, I guess I have to put my hand down because I don't have a comment for that.

JANIS KARKLINS: Again, as I said, maybe we are a little bit tired and we need some time to reflect. Maybe a way forward would be to ask staff to consider, in light of the conversation, what we had on the topic conceptually and in light of proposals that have been put forward to try to draw and propose a possible way forward for our consideration for the next time we will look at this language. So that's where I'm heading.

Now Brian's hand is up and Alan Greenberg's.

BRIAN: Thanks, Janis. I'm getting a better sense of what we're trying to do here. It's starting to feel like we're not looking at Article 9 special categories of data but other things, like Laureen mentioned, that should factor

into the balancing test. So that might be a better to frame this conversation and I think might get us to where we're going.

I wanted to poke on what we're trying to accomplish here, too, in that the way that the language is drafted it says we must not disclose non-public data in these circumstances. I think that's part of what's giving us some heartburn because, if that entity has enough of their own issues as a subject of phishing attack or a DDoS attack or a malware infection, we can't tell them about it? We can't contact them and that data can't be disclosed to someone who's trying to help them? I think maybe "must not disclose" is not the appropriate objective here but that the request really needs more scrutiny or should be treated differently. So I would offer that additional perspective. Let's be clear about what we're trying to do and then do that. Thanks.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. I support what Brian just said, but I also look at it and say, "Yes, maybe you'll recognize it." You may recognize Falun Gong as a sensitive thing in China, but someone else who doesn't read the news may not. It's just so subjective to say you must not do something based on cultural issues and all sorts of issues. Again, I have great problems imagining how one can implement this kind of thing reliability or say your subject to penalties if you don't. You might not recognize it when you see it, despite what the Supreme Court judge said.

JANIS KARKLINS: Okay. So, not easy. Let us sleep over it. As I mentioned, I asked staff to consider and maybe come up with some proposal after the analysis of what everyone said, including doubts of implementability of the principle but also existing formulations. So we will give it another try. If that other try will be unsuccessful, then probably we need to take a note, either a formal note or mental note, and then move on. But we will still give it another try with this concept.

With this, I think we close some issues, but this building block still remains in yellow. We will revisit it as we will be ready to do so, partly maybe during the meeting here. When it comes to – what was the numbering? The previous one. H? Or …

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: The upper one.

MARIKA KONINGS: H.

JANIS KARKLINS: H. So that we will revisit once the overall concept of the SSAD will be clear.

Thomas?

THOMAS RICKERT: I was thinking about yet-alternative language. I know that you want to move on, but if I may suggest one sentence because I think we're trying to capture different things. To a certain extent, I think we've been talking past each other as to what the problem is that we want to solve. My take on this is that, wherever the circumstances of the disclosure request or the nature of the data to be disclosed suggests an increased risk for the data subject affected, this shall be taken into account in the course of the decision making. I guess that would cover everything – the legal organization-type thing, as well as special categories of data – because, if we use language that is too specific, we might lose things. I think all we're asking for is [inaudible] standards for balancing developed and that special attention is paid to this.

UNIDENTIFIED FEMALE: [inaudible]

THOMAS RICKERT: [inaudible]

JANIS KARKLINS: Okay. Could you send it over?

THOMAS RICKERT: I will.

JANIS KARKLINS: My proposal still stands. We're maybe slightly tired now. We will have fresh look of this specific – not on H but this specific J – maybe tomorrow or on Monday. Then we'll see whether we can nail it down or leave it. Thank you, Thomas, for your proposal.

Let me now suggest that we move to the next building block: query policy. If I may ask to put the query policy on the screen. Query policy consists of also two parts, one related to the entity disclosing data and another one. Let's take Building Block I, related to the entity disclosing data. In Point A, the unresolved issue remains the abusive term of use of nature. We discussed that the list of what that may include could be added. This is now what you see on the screen. I open the floor for comments.

I have Mark Sv and Alan Greenberg. Is it on this one?

No? Maybe Caitlin will introduce …

CAITLIN TUBERGEN: Thanks, Janis. I just wanted to note what has changed since the last time we discussed this as a team. If you might recall, we talked about the concept of proportionality. Under #5, you'll see bracketed text that says, "When investigating abuse based on this specific behavior, the concept of proportionality should be considered. For example, the threshold for high volume may greatly differ based on the size of the registrar." But all of the other numbers under abusive use have remained unchanged.

JANIS KARKLINS: Thank you, Caitlin, for this clarification. Any comments on the list of abusive use?

I have Alex Deacon and then Volker. Alex?

ALEX DEACON: Just two things. On the definition of "abusive" there, the starred asterisks, when we use the phrase "but is not limited to," it always raised a concern to me because it could blow away this principle of predictability. I'd rather see a more definitive list and not have it be open-ended. That's my one concern on that.

On Point 5, just to address the issue that Caitlin just mentioned, we really can't answer that question until we know who the decider is. So, once again, we're chasing our tail. So I think we leave it as bracketed and don't spend much time on this until we have something nailed down. Thanks.

JANIS KARKLINS: Thank you. Volker, please?

VOLKER GREIMANN: Thank you, Janis. I am a bit worried about all kinds of attributions of intent – for example, in number five, "with the intention of" and formulations – as they would require evidencing the intent of a third party. We should limit it to actual actions that can be evidenced without

requiring attribution of intent. If you do that, if you cause SSAD or other parties to fail SLA performance, you're using it in an abusive manner not matter what your intent was. That would be the right way to approach this. We cannot go into attribution of intent because that leaves wiggle room that everybody will use to say, "Oh, I didn't intend to do that."

JANIS KARKLINS: Thank you, Volker. Margie?

MARGIE MILAM: I think I have the same concern that Alex has. It depends on who's the disclosure because some of these things I think I'd want to really go into if its not ICANN. Frequent duplicate requests that were previously fulfilled or denied … There could be a lot of back and forth between if it's a contracted party and the requester on "I need additional information" or there hasn't been a response. So I think this is probably a little too broad and could be misused.

JANIS KARKLINS: Greg, please?

GREG AARON: Thanks. Number 3 is a concept that is applicable in anonymous public access, but it's an apples-and-oranges thing in a system like SSAD, where access is going to be controlled and the users will be known. We don't know if there are going to be quotas in that kind of thing yet at all.

My suggestion is to delete it because I think the abusive things that people are worried about are going to be covered under other language.

6. I think we're all good on the concept. This comes out of companies trying to just mine stuff. "Mine" or "harvest" are probably undefined terms. I think we would probably use it because if you're in this system, you're going to making legitimate requests and you're going to be able to demonstrate why you're doing these requests. If you can't, those are illegitimate and you'll get kicked out.

So I don't think 6 adds anything. It's a little vague. 3 we probably should talk about deleting.

JANIS KARKLINS: Stephanie, please?

STEPHANIE PERRIN: Thank you. I am up above in a response to "An SSAD request must not include more non-public data elements that have been requested by the requester." I'm wondering where this came from. I actually thought I had intervened and killed this off a while ago, but clearly I didn't. In the event that you have a novice requester – say, the average citizen that we're always talking about who needs this data for consumer protection – they may not have a clue on what data they should be asking for. In that case, an informed registrar looking at the purpose statement and the request might say, "Okay, here you go. Here's the

packets you need." I don't see why we should stand in the way of that if it's a legitimate purpose and a legitimate request."

Furthermore it says, later on, conversely, "The response must not include the public data elements." That was the part I thought I'd killed off. Why not? Why not have a complete request at the same time? It's an RDAP request. You're not killing any trees or anything. Why not have it all at the same time? What's the rationale? Thank you.

JANIS KARKLINS: Sorry, Stephanie. For the moment, we're talking about A, not in general but specifically Sub-Point A. That's why I didn't follow your comments.

STEPHANIE PERRIN: Yes, I'm sorry. I'm out of order. Sorry.

JANIS KARKLINS: Yeah. We're still on A and the list of abusive users. I have a long list of requests. James, Mark Sv, Alan Greenberg, Volker, and Milton. James, please go ahead.

JAMES: Thank you. As the author of this list, I just want to first note that it came before some of the other dependent changes that we have since made. Some of these things have been overtaken by edits. So I want to put that out there.

Secondly, we discussed this and I was asked not to come up with an exhaustive list but a specifically non-exhaustive list for examples. I think one of the comments is that there's not enough specificity here. That was part of the assignment.

There was also a question about whether or not a back-and-forth exchange between a request that was not fulfilled would constitute abusive behavior. I think it was pretty clear here that it was duplicate requests that had been denied. So it wouldn't be a duplicate if it was changing or information was being added or removed, and it would not have been denied if there was no response issued. So we're specifically talking about asking a request like, "May I have this data?" "No." "How about now? … How about now? … How about now? … How about now?" This is the type of behavior that we consider to be abusive, and it would not encompass those types of interchanges where more data was being requested and the request was changed but necessarily fulfilled.

So that's where ended, but a lot of this stuff was present and identified as abusive use of the previous system that SSAD will replace (the WHOIS system). So I think, if we feel like it's cutting a little too close to home, then maybe we can pull it back a little bit. But that's where this came from. It wasn't necessarily pulled from thin air. Thanks.

JANIS KARKLINS: Thank you, James. Mark Sv?

MARK SVANCAREK: I think number three is just a variation of number three. The intent of number three is to say, "I am pretending that I am multiple people instead of one person in order to get around some sort of quotas or rate limits." I don't think it's going to be applicable to our future system. So I think ultimately number three is gong to go away, whether we get rid of it now or later. I think the way to look at it is, if I'm using VPNs, will my use be considered abusive under number three? So just something to think about there.

I do agree with Volker that we should be tracking against observable behavior as opposed to implied intent. That was always my objection to number six. You're assuming that the disclosures are for the purpose of mining or harvesting, which is another one of these "I'll know it when I see it" things that I don't like. So I think that's a real big problem with number six.

With number five, if you fail the SLA, then that's automatically considered abuse. But also SLAs are dependent on the size of the registrar. I don't see how that could possibly work. That just seems like somebody will poorly provision themselves and then declare that behavior as abusive because they can't keep up. So we're going to have to work on five. I don't see how it could possibly work as it's written right now.

But number six, if we're focusing on observable behavior as opposed to implied intent, I don't think can survive either. Thanks.

JANIS KARKLINS: Thank you. In the meantime, technicians, if you could check the microphone. Alan Greenberg, please?

ALAN GREENBERG: Thank you. You took away my request to buy Mark a new microphone, but thank you. I have a problem with number two. I'm not sure if it's simply omitting words. For instance, if Mark asks for something and it's denied or granted and I come back a day later and ask for it, is that abusive? I don't have a clue what he did. So I'm not sure if the intent here was from the same requester or not. So I think we've got to tighten up this kind of language if we're going to class someone as being abusive for things they have no control over.

JANIS KARKLINS: Noted. Volker?

VOLKER GREIMANN: I would like to raise a couple of counterpoints to some of the arguments that I've just heard. First, to number two, we see a lot of those requests where we get the same domain name requested by two different parties acting on behalf of the same requester that has availed themselves of multiple services, therefore causing load on the system that's not necessarily. So I think a requester should make sure that the number of requests is limited to the bare minimum and that multiple requests are filtered out at the requesting stage, not at the stage of the response. If we see those, then there has to be a limitation.

Number three. It's very easy to set up a new company that could get accredited. Just ask Donuts how they set up their gTLD applications for legitimate purposes. But it's also possible to do that for illegitimate purposes. Set up a hundred companies. They all get accredited. Then shoot off the requests. Once you find out they all belong to one person or one entity, that's abuse.

Number five. No, it's not a question of, if you fail your SLA, then it was abuse. But, if you fail your SLAs because one or two parties overload your request queue and you fail your SLAs just because of those two parties sending in high loads and high amounts of requests, then there's a high likelihood of abuse.

Finally, for number six, this is a problem that we have seen in WHOIS in the past that led to large spamming campaigns and abusive use of WHOIS data. It's natural that we'd like to prevent that in the new world, that using the access to obtain this data for malicious purposes should be prohibited. For example, if we see spam that goes out to our registrants and we have seen requests coming in before that, then that is clear evidence that the requester has used that for their purpose, and therefore he's kicked. This is not rocket science. This is based on observable behavior that we have observed in the past. It's natural that we'd like to see the system protected against that.

JANIS KARKLINS: When this request was formulated to James to draft a non-exhaustive list of possible abusive behavior, it was meant to help us proceed and get over or agree on Sub-Point A. There should be limitations if there is

obvious abusive behavior. Now the list itself has become a problem, so maybe we should simply accept the general notion of abuse behavior and not spend time editing what potentially is this abuse behavior and leave it vague as a policy because sometimes it's better not to say. It's just a suggestion because I've seen that, in trying to avoid or overcome one issue, we have created a huge problem. So just a suggestion.

I have Milton, Brian, Mark Sv, Alan Greenberg, and Greg in line.

MILTON MUELLER: Let me just first quibble with what you just said. I don't think we've created a huge problem. I think we are protecting ourselves against the potential abuse of this. There are people who, for one reason or another, are afraid that that will limit what they plan to do, I guess.

The issue of "non- exhaustive includes but is not limited to" is of course a perennial problem in these kinds of exercise, but I think some kind of a definition is necessary to protect good-faith uses that might be perceived as abuse by somebody for the wrong reasons. I think, by setting out this many very specific examples of what is abusive, we create a pattern and a generality that could be applied to things that are not listed but would not be overly board. So I think it's the right approach to have this kind of a list.

I'd particularly like to weigh in on number six. I think that's one of my main concerns of abuse: people will use the SSAD to essentially go out and harvest or collect repeated data and build up an independent database so that they can bypass the actual process of individualized

disclosure. I think that's clearly something that certain people would have an interest in doing.

I think we could do a better job of defining harvesting or mining. I could give that a shot. Not now. My brain is numbed by eight hours of EPDP. But, yes, I agree with Greg that we could do a better job of defining this, but I don't think we're describing an intention here. I think we're describing a patter of action. So I would definitely not want to delete this on that basis.

But, really, on the whole, I think, if we want to maintain some credibility, we can't through out the whole concept that there could be abuse of this and that you need to try to define abusive behavior. I think we have to do that. Thanks.

JANIS KARKLINS: Thank you, Milton. Brian?

BRIAN: Thanks, Janis. I have one cheeky comment for Milton and one constructive suggestion. The cheek comment is, for one reason or another, we want this because today we're being rate-limited to an extent that's not reasonable for legitimate requests. SSAC noted that in SAC 101. So that is why it's important. I'd love to along with Janis' suggestion that we leave this in more general terms of "You got to watch out of abuse in the system and take action." But that rationale has prohibited us from doing our job in the past, so that's why we want

specificity in what abuse is: so we can't be denied for non-abuse reasons. So that's where we're coming from there.

The constructive suggestion I just wanted to add, in addition to thanks to James for putting this together, is that, if we remove the part in Point #5 of "or other parties" there, then we can remove the brackets there, too. What we could arrive at is a bullet that prevents the intention of causing the – I don't like the "intention" part either – SSAD to fail SLA performance. What that does is that leaves the SLA on the contracted party – between them and ICANN or them and the entity who's running the SSAD. The entity that's running the SSAD won't have any beef with the contracted party about not meeting SLAs because that party who's sending them the request will know how many they're sending them. If that party is overwhelming the contracted party with request volume, they won't have a leg to stand on to say, "You're not meeting your SLAs," because they'll know they're flooding them.

So I would remove those three or four words there in number five, and then the bracketed text can go, too. Thanks.

JANIS KARKLINS: Thank you, Brian, for your proposal. Mark Sv?

MARK SVANCAREK: Volker, thanks for clarifying what was meant by number three. I understand now. I still think that that's either a variation of number four or it's something like a failure of the accreditor, that the accreditor is

giving out multiple credentials to the same entity. But at least now I understand what you're getting at.

I like Brian's idea that the SLA should be the SSAD SLA because I really just don't want to take a dependency on small registrars crying foul because one day there were a lot of names that needed to be pulled from them.

Let's please, on number six, attempt to better define mining and harvesting. I know to some people it seems like a very obvious concept and we all understand what happened in the past. But, if we are attempting to do good-faith usage of the system, I'd like to know really clearly what I'm allowed to do and what I'm not allowed to do if I have any kind of volume at all or if, for various reasons, I'm required to retain data for a period of time. So, if I have to collect a collection of data that is somewhat large and if I have to retain it for a period of time, I don't want to be accused of abusing the system because that has a superficial resemblance to mining or harvesting. So we do need to clarify those terms. Otherwise, I will never be comfortable with them. Thanks.

JANIS KARKLINS: Thank you. Alan Greenberg, please?

ALAN GREENBERG: I think we need the overall provision here. I find examples useful, but I think we need to be really careful. If we don't have the examples at all, then clearly people will have very different views and will have very

different enforcement rules when things get down to the contracted parties. I think we have to set some high-level principles above that.

On things like mining and harvesting, if we're setting rules saying you must have a reason and you must only use it for that reason and someone is requesting 100 million or a good fraction of 100 million domain names, chances are pretty good that they're misrepresenting themselves and we can get them on those rules. We don't necessarily have to have a harvesting and mining rule explicitly.

So I think I need to be really careful that we're not going to identify legitimate use as one of these abuse. At the same time, there are people who are going to try to abuse and we need to have provisions. But we want to do it in a way that as little as possible will impact the legitimate users. Thank you.

JANIS KARKLINS: Again, I would like to come back and invite you to use simply common sense. What is the possibility that someone will come and ask for a million domain names? What would be the legitimate purpose of somebody asking immediately for the disclosure of private data on a million domain names? Hard to imagine, at least in my mind. Do you have an immediate example?

UNIDENTIFIED MALE: Yeah, Janis, I do. But we, Mark Monitor, has brand protection clients that have, at any given time, a hundred thousand domain names that we've identified as infringing that have content that's doing something

malicious and that we might need to check if we're going to do a report for the client or check to see if the bad guy still owns the domain name. So it's foreseeable that, for any given client, we might have a seriously high volume that we would need to check at a given time.

JANIS KARKLINS: Okay. Then that's simply my inexperience in that area. Or ignorance. Let's put it that way. Sorry for that. Greg, please?

GREG AARON: There are criminal entities who consume hundreds of thousands of domains over time. Of course, the problem is you have to figure out which of the domains are theirs. You can deal with those. Sometimes you're going to have a query a number above that to figure out and winnow the bad party from some innocent parties as well. So hundreds of thousands is a pretty usual situation. It happens every once in a while.

I think we area arriving at maybe consensus on the idea that having a list is a good idea because it allows the participants in the system to have a common understanding and reduces the ability to have loopholes that people don't understand. So I think having the list is a good idea and we can probably fix up the list.

One question. Otherwise, who does decides what's abusive? If we just have a general principle, who decides? I don't know. If you're interpreting a contract or a policy, there are two sides and they're going to disagree. So how do you figure that out? That's a problem we have

right now with rate-limiting. Somebody says, "Well, one a minute. That's my policy because that protects my system," and other people say, "I can't use this system to do what I need to do for legitimate purposes." So we don't want that situation to happen again.

JANIS KARKLINS: I think that ultimately that is the decision of the one who does the decision on disclosure. We have in reality two major options here. Either that is a centralized authority that does disclosure – maybe ICANN – or that is the 2,000+ registrars who make this determination. Then, of course, each of them would make a determination on whether that is abusive or not. So I think that's simply common sense that suggests that type of an answer.

My question is, is there any way that a group of three or five could come together and work on this list of abusive behavior? Is there any volunteers who could do it by tomorrow at 5:00 in then afternoon when we have our next meeting? Can I ask, is there volunteers? Raise hands.

Milton is one. Margie is one. No, no. Just volunteers from the registrars/registries. Volunteers, we need you in the game.

UNIDENTIFIED MALE: We took our best shot.

JANIS KARKLINS: Okay. That's you. So we have now identified. Is there anyone from SSAC being part of the smaller team? Yes/no? Volunteers?

Okay, Ben. Thank you for volunteering. So I would say, Margie, James, Milton, and Ben, if you can find –

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARKLINS: What's the …

MILTON MUELLER: Yeah, I heard James volunteer.

UNIDENTIFIED MALE: Let the chat record show that James specifically un-volunteered.

JANIS KARKLINS: Ah. Okay. So who volunteers from the contracted parties side?

MILTON MUELLER: A motion to conscript James.

ALAN WOODS: Genuinely, I know we are all pushing this, but this is a very, very full meeting. I genuinely can't commit to it and I don't think a lot of us can commit to it. We just don't have time. I'm sorry.

JANIS KARKLINS: Without you, probably it will be a failure.

MARIKA KONINGS: [inaudible]

JANIS KARKLINS: Okay. Can we stop now and ask—

[JAMES]: I will volunteer as tribute.

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARKLINS: Okay. So let me then make a suggestion. We stop here and we ask four or five people, including myself and Marika, to gather around here and try to work out the list that could be within the next 20 minutes. The rest we will let enjoy sunny Montreal.

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARKLINS: Alan, please?

ALAN WOODS: Sorry. Just reading this list, there was something I just said to my registrar colleagues: I feel like we're looking at this list somewhat backwards. We're looking at it as if it's a list that shall be policed as opposed to something which is akin to an acceptable use policy, whereby it's not a sword. It's a shield. Therefore, if an action must be taken and is assessed in an individual situation, this list will give the ability where it has confirmed being malicious to be something that is dealt with. We're not saying that in every single instance, where you might have a fringe case where you have to do those. An explanation is more than enough to see this clearly wasn't abusive. But if it was in an instance where it was abusive, then this list would then apply. It doesn't need to be seen as something that is necessary, as I said, going to be policed but that there is elements where we need to consider that it could potentially be a reason for abuse.

So I would just caution that we're not looking for exact here. We're looking for breadth more than anything.

UNIDENTIFIED MALE: That's very insightful. Sounds like someone wants to write a list.

JANIS KARKLINS: I would say it is now. Let me take just Hadia's comments and then we will break.

HADIA ELMINIAWI: My problem here with creating a new group to come up with a new list is that I don't find, actually, a problem with the list because most of us here do agree that, if those practices are proven to be true, then it's not acceptable. But our problem is not with the practices. Our problem is with the implementation and the detection. How do the registrars determine that such an action happened? I think the problem here lies with legitimate requests being mistaken as abusive requests. I think this is the problem that we need to address. How can we ensure that the way the registrars detect this action will lead to accurate decisions about who's abusive and who's not. Maybe you can try putting together some other group to come again with some other lists, but again, the problem still exists. I think this is the main problem here.

JANIS KARKLINS: Thank you. We agreed that there may be some measures to be put in place to make limitations in numbers, but when? What are those circumstances? We agreed that this might be in the case of abuse of the system. So now we're trying to identify what those abuses of the system might look like. Alan, I think, suggested a very good way forward, saying that we need not to describe exactly what it is but we need to come to the common understanding that this may constitute abuse of the system, which then would allow us to consider putting some kind of limitations. So that's the crux of the matter.

Now, when we are discussing, we hear different opinions about this non-exhaustive list. The point is we would try to fine-tune, not create a new list but simply fine-tune what we have among those who are most

interested. Hopefully, if those who are most interested could come to agreement, then the rest would say, “We’re fine with that.” So this is the proposal from my side.

Thank you, volunteers. The rest of the team are relieved. Volunteers, please gather around this side of the table. Thank you very much for your constructive approach during today. I understand this was a long day. My apologies for that. But I’m very happy that we closed the accreditation block, except the part that will come from the GAC that we will address on Monday, hopefully. With this exercise, maybe we will get to the list of what we could consider as potential abuse of the system. We will meet again tomorrow at 5:00 for a session which will be 90 minutes. We will continue the discussion of the building block on query policy.

Thank you very much. We can stop recording. To the group of volunteers, welcome to this side of the table. To the rest, have a good evening. See you tomorrow at 5:00.

[END OF TRANSCRIPTION]