ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 1-PM
Monday, 27 January 2020 at 16:00 UTC

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

JANIS KARLKLINS: This was the message [that I] heard. But I was expecting it. So thank you.

We finished the meeting talking about the model, and it seems like we converged on the model which staff will try to describe and present the write-up of sometimes tomorrow.

But what we still need to talk through in this evolutionary model is whether we need any kind of accompanying body/mechanism which would assess exchange experiences, lessons learned, and improve the functioning of SSAD over a period of time. So that's the question.

Initially, we proposed a steering committee, and that proposal was not received overly well, mostly I would say because of then proposed composition. In subsequent conversation, it turned out that the idea of a mechanism – whatever we will call it ultimately – might be something to think about. Certainly, the composition of that mechanism needs to be also worked out at one point.

I would suggest that we maybe brainstorm at this point and think of how that mechanism would look like. What would be the functions of that mechanism? What checks and balances do we need to put in place, making sure this mechanism would not venture into policy development in any way? Is there an already-existing mechanism could be used to assess how SSAD is working? How do we ensure consistent with the role of PDP and requirements and contractual arrangements. How do we avoid create a lot of overhead while ensuring the diversity of use and balancing of decision-making within that mechanism? Should there be any kind of supervisory of any other bodies? The first that comes to mind is the GNSO Council in the work of that body. So these are more or less questions that we formulated just to stimulate this conversation about the potential mechanism. So we started a little bit in one of the calls, but this was very limited. We thought that this would be important now to exchange views.

Based on this conversation, which probably we would have for about half-an-hour or 45 minutes, staff would try to capture the essence and then propose something in writing for our further consideration.

The floor is open.

I have Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Thanks, Janis. I had a little bit of a chat about how some of the suggestions around the model would impact a group and what that group would look like. One of the first things we talked about

really was, if you have this centralized system that does the recommendation to the contracted parties, then there's some learning to be made there. That learning would then change where the decision might be made – whether that is automated or whether that goes towards a centralized system. Really, when that happens – Stephanie might love me for this, so I'm just waiting for a thumbs up – realistically, DPIA is going to changed because you're changing your whole processes. Really that's a process that'll have to take place between the contracted parties and ICANN, if ICANN is that central gateway. So that will change how the system works – a DPIA.

Then you'll have some sort of joint controller agreement, [inaudible] or whether it's a process[ing]. I'm not going to go down which one I think is right or wrong. But that obviously also needs to be changed. Realistically, we're not changing policies here. We're making decisions based on impact assessments and controllership agreements. So not policy. Just making that clear. It's a change in how the system works and who is the responsible party for making certain decisions and how those decisions are made.

So realistically – this is literally my views; this is brainstorming here – I think that's a decision between contracted parties and ICANN. They're the two – they have the data – that make the change. However, it obviously impacts the whole system, and this where we get to the checks and balances.

Really my or our feeling is you probably just take one person from each of the groups that are represented here and have it as a public comment for that group to say, "These are the changes that

we're making to the DPIA," or, "This is the analysis from the DPIA. This is the changes to the joint agreement. This is our reasoning. Does this make sense? Is there anything that we haven't thought about? This is a complicated system and everything else that impacts everything else. [Over to your] review team for our changes to the joint controller agreement. Is that correct? Let's move this forward into the model."

So that's my initial thoughts on how that would work here. Because it's an agreement or change to the joint controller agreement, we're not talking about a massive group that's going to have decisions to be made. The decisions are based off the analysis from the DPIA, not from what a single group thinks. It's from analysis that's been carried out from legal information that has come in and from experience in the system. Thank you.

JANIS KARLKLINS: Thank you. James followed by Georgios.

JAMES BLADEL: Thanks. Thanks, Chris. I think that was a good way to kick us off. This is going to sound cynical and negative, and I understand it's brainstorming. But I promise it gets better. So if you could just give me a little bit of rope here. I'm just looking at the list here, and the list to me reads like something that, in every working group – I've been doing this now for over a decade – we all say we agree needs to happen and we are so very bad at everything on this list. I'm thinking of the transfer policy and all the different ways we tried to make that an iterative process. Or we can look at the New

gTLD Program, where the first round took for four years, the second round took eight years, and now we're into a decade. We're getting worse at putting these things out. We actually are making things so hard that eventually the next round after this will probably take 20 years. It's like building a cathedral or something. Somehow we actually get worse at our jobs the more we do it.

And, when we talk about this mechanism, you will see the defenses go up over here in the contracted parties. Why? Because we sign a contract that says we will do what ICANN says in advance without knowing what that is. We put some guardrails around it – a picket fence or whatever – but we have this contract hanging over us that has all these blanks that could be filled in. We essentially [are] handed a blank check and say, "Go ahead. We'll cash it later." So it gets very nervous about delegating that kind of authority to these unknown bodies where it's not clear how they're going to be composed or comprised and how they're going to operate and what's in scope of their remit. So that's where you see the defensiveness.

But, that said, I think there is some merit in pursuing this idea. But we have to just recognize some of those limitations. For starters, it should probably be what Volker is saying: more of an advisory capacity to say, "Here's what we're learning. Here's what we're finding. Here are some relevant court decisions that were not available to the EPDP at one point. These can feed into a process."

The second thing is that we can use an existing process, if not the PDP. We could use, as Volker pointed out, the process by which contracted parties can voluntarily adopt amendments to their

contract, which then becomes enforceable by ICANN Compliance. Now, this is a high bar where you either have to have a majority of them vote or you have to have a super majority of domains under management. So that's a certain number of registries or registrars, but it is possible.

Of course, the GNSO could be the referee or the umpire that calls balls and strikes by saying, "This is implementation. This is policy. This can go through this advisory board, and this can't." That could be this oversight mechanism over that.

The bottom line is that this is an idea worth pursuing, but you have to understand that the reason for the limitations are not just reflexive opposition to the idea. It is a concern that the contract is already fairly open-ended and introduces a lot of uncertainty. And this magnifies that uncertainty.

Anyway, I just wanted to capture one other thing that Chris said. There's going to be a lot of these privacy-related things as regulations grow and evolve. ICANN I think in particular has to have certain officers on staff. They have to do these DPIAs going forward. This body could do all of that. It couldn't be just limited to fixing this policy but it could be taking all of that on board – all of the legal conflicts/conflicts of law. All of the changes associated with the privacy landscape could feed through this representative body of experts and then percolate out into policy implementation or even changes to ICANN org. Thanks.

JANIS KARLKLINS: Okay. So here we have now proposals for a [name] advisory mechanism.

Next is Georgios, followed by Marc Anderson.

GEORGIOS TSELENTIS: Thank you. I just want to highlight something here that I think we should not forget regarding when we talk about SSAD evolution. We have to see an evolution which is happening in terms of more practical issues that will help streamline the existing policies. If we are talking about changes in the SSAD that touch to the core of the policies, I think we cannot avoid that we need the opinion of the controllers who decide the purposes for which we are doing the processing activities. Therefore, I think somehow we need to clarify when we talk about SSAD evolution what level of evolution we are talking about.

As Chris highlighted, if this evolution is referring to [what] an impact assessment is saying, then probably we can do with a more flexible and more participative group that can do this. But, if we are touching to the hard core of the purposes, for example, of processing and we are changing some things on this, then we cannot do without consulting the whole group that does so. Now, what sort of representation? That's another story, but I think we should be careful of that.

JANIS KARLKLINS: Thank you. The idea is not to design this mechanism which would not touch a policy development, which may to come to a conclusion that some changes in the policy development process

need to be initiated and then send that information to the GNSO Council to initiate the new policy development process but not venture into policy development itself. The mechanism should assess how SSAD works, and we should discuss what works and what doesn't and whether any improvements could be made, including on the level of automation and so on. These are very practical things making sure that the whole system functions properly.

Marc Anderson, followed by Brian. Marc, please?

MARC ANDERSON: Thanks, Janis. I think everybody that has spoken so far had some very thoughtful and productive things to say, so I think we're starting off the conversation from a good place, which is encouraging.

One of the things I raised my hand to react to is that you mentioned if existing mechanisms be explored. I think yes. I think, before we invent a new mechanism, we should be sure that existing mechanisms aren't sufficient.

One of the things that we've talked about a couple times is that we certainly have the ability to leave things to implementation, but what we found is that we need to be very clear, when we're leaving something for implementation, what we expect staff – staff ultimately has responsibility for implementing the policy recommendations – to do.

So I think there are some opportunities where we can instruct staff in what we expect them to implement, what decisions we expect

them to make, and maybe what decisions we expect them to review over time.

We have a policy review process, an existing process that exists within the GNSO, [creating] procedure. So I think we need to be very clear in understanding where that can't work, that we're needing this additional, supplementary recommendation. I think we'll have to be very clear on what powers this review team, what's in scope, and what's not in scope of it – whatever we end up calling this body.

So that's my input at this point.

JANIS KARLKLINS: Thank you. I think that this is our task: maybe to define the boundaries of the scope of this group. That would fall within the policy development process.

Brian, please, followed by Stephanie.

BRIAN KING: Thanks, Janis. Marc said very well what I wanted to say on quite a few point, including to look at what we have before we reinvent the wheel, especially because we need to move quickly. So, if there's some mechanism already in place that's tried and true that we can put this into with parameters that we should decide as an EPDP team, then we should do that.

If I'm reading between then lines or guessing correctly, I feel a concern from our contracted party friends, and they're right, I

think, to have this concern: that the policy we develop today shouldn't be changed out from under them. So we don't want to develop a mechanism to undo or redo or change that once it's developed. So I think we can do a really good job of that by giving that group or that mechanism clear remit and clear marching orders, and that should be the key to success in doing this. I think it can be done because we can be that clear. Let's do it that way. Thanks.

JANIS KARLKLINS: Okay. Stephanie, please?

STEPHANIE PERRIN: Thanks. My first comment would be, while I don't believe in replicating structures, we don't have enough people to staff them. The IRTs have a pretty long history of fairly siloed existence. We have several siloed IRTs whose work they're trying to implement has been [inaudible] by the GDPR. So they're on hold. The PPSAI is one, and thick/thin transition is another. And there are several WHOIS-related policies.

So my message would be that there has to be a holistic approach to the inevitable changes that will be coming as the law and the precedent evolves. So I like Volker's privacy council name, and it has got to look over all aspects of this.

Now, I think it might be instructive just to take a hypothetical to see how this would work in the structure that Chris was outlining. Thank you very much for the notion of a DPIA because that's what we really need. Let us take the legal opinion that we are

requesting on the matter of the recent Google decision that throws up in the air the concept of extraterritorial application of the GDPR. There are some parties here that would definitely like to adopt a more conservative approach to the extraterritorial application of the GDPR. That's a big policy decision. That's not an implementation decision.

So let's imagine that decision had shown up a year from now after we have this thing all in bed and working beautifully, and we have our oversight committee. An individual group who wanted to have a change in policy to reflect the precedent that their legal advisors tell them gives them at least a reasonable risk that they feel ICANN not to be taking takes it to the committee. You do a full DPIA. Yours truly would argue for a human rights impact assessment because this, of course, has implications under the charter as well and various other legislation that applies in the different jurisdictions – also competition. So you really need a broader look at the thing. Then is a committee is struck to review all that, and then it goes back to the GNSO Council.

One of the, I think, [besetting] problems here – I did sit on that Policy and Implementation Committee that I know Chuck Gomes was on (can't remember the other guy); it was a good committee and we sorted out this fight over what's policy and what's implementation – is it's a lot harder when we're talking about legal precedent. Some legal precedence might just be tinkering with the input from the SSAD – a data element here or there of something. If something is determined to be not readily releasable, well, then we might have to shut something down. Others are more a fundamental policy shift.

So I think we have to take that apart a bit and be aware that the determination of policy and implementation is not going to be so easy in this, in my opinion. Thanks.

JANIS KARLKLINS: Thank you, Stephanie. I was trying already to start writing in bullet-point format what would be the scope of this mechanism, so I would invite people to come up with further bullets or further functions or argue against ones that are on the screen.

The next is Margie, please.

MARGIE MILAM: Talking about existing structures, I just want to remind folks that the RAA has something about a code of conduct for registrars. There's a procedure in how to get that implemented. I think it's a majority of registrars in the stakeholder group or something to that effect. I don't know. That's one area where you could pull it into the contracts in a way that's outside of, say, for example, the GNSO.

JANIS KARLKLINS: Marika, please?

MARIKA KONINGS: Thanks, Janis. Thinking as well about Marc's suggestion of using existing mechanisms or procedures, I don't know either if one alternative approach – also factoring in that people don't want to create a lot of overhead but still allow for the free flow of

information – something like an open review of the policy, could be a mechanism.

As you may know, as part of the CPIF, the … I don't even know [inaudible] but basically the framework for implementation. Recently as well staff worked on a predictable process for how reviews are conducted. I think you've seen with the transfers how that worked, where basically org from its side writes up what their experiences with the policies are, what kind of complaints they've seen, and what changes may have happened in the broader landscape that gets published for comments to ask as well the broader community about their experiences. Basically, based on that, it's turned back to the GNSO Council to decide how to move forward or what the potential options are.

So I'm just wondering as well if you could have something as an open-ended review, where those that have new information can provide it in a very open channel while org can then also from their side share what their experiences are, statistics they say, and potentially as well recommendations coming out of that and bring that back to the council, where then, of course, a conversation could also be had directly with contracted parties – what path can be followed to make these changes in an expeditious way but also an assessment of what our policy-related questions are that would need to follow a different path. I don't know if that finds a little bit of balance between having an open mechanism where the constant feeding of new information and suggestions can be provided without having each group need to appoint someone and someone needs to support that group as well but have it more driven from a kind of continuous review perspective that is able to

then channel whatever comes out of those conversations or the input provided to the respective process where changes can be made. As part of that, I think it needs some of the options, as Margie suggested, which could then as well be proceeded as part of that conversation. “Here are some changes. Here you can implement in either this process, that process.” Or the other GNSO contracted parties discuss and decide what’s the best path forward.

JANIS KARLKLINS: Margie, your hand is still up?

MARGIE MILAM: Sorry.

JANIS KARLKLINS: No, it’s an old one. Anyone else?

I didn’t get a sense of whether we’re going in the direction of existing bodies or proposing a new kind of mechanism. But whatever it is, before we decide, we need to think more about functionalities. I started writing on the board what I heard that could be functionalities of this mechanism with the understanding that there would be a supervisory function of the GNSO Council. And there would be interaction on a periodic basis with the GNSO Council of that mechanism.

So my invitation, in absence … No, there are, but still my invitation stands. Please feel free to come to the, while you’re walking

around, board and then write any other functionality you think this mechanism should do or edit what is on the screen.

At the end of the day, we would make a picture of what is on the screen, and staff will try to do a write-up of the scope of activities of this mechanism. Once we will have this clarity or at least idea of the scope of the mechanism, then we can think through whether this scope could be entrusted to an existing mechanism or we need to propose a new one.

I see Thomas' hand up, and there was also Marc's hand up [inaudible]. Thomas, please?

THOMAS RICKERT: Thanks very much, Janis. I have a question with respect to this group. Have we given up on the idea of presenting our findings to the authorities as a code of conduct to get legal certainty for all parties involved? Because I still have that as a goal in mind, that, since a lot of folks have asked for legal certainty, we would translate our policy recommendations and potentially the implementation thereof into a draft code of conduct, get that hopefully approved, and then everybody who plays by the rule of the code of conduct will be safe.

Then another role … If we still think that this should be pursued, then this group could also work on overseeing the drafting of this application and liaise with the authorities because I think we need somebody at the steering wheel to take this process further. I think it would be liaising with the authorities on a code of conduct and also a subset of that group to liaise with the joint controllers who

might need to make adjustments to the agreements that are hopefully in place by then based on that exchange with the authorities. I'm looking at Georgios, but I think there might be feedback from the authorities that we need to make changes to the existing system. I think this group could be a good catalyst between the community/GNSO Council and the joint controllers to drive this forward.

UNIDENTIFIED MALE: It's a cost-cutting exercise, Janis, with …

JANIS KARLKLINS: Again, please feel free to come to the board and scribble your ideas for further consideration.

I have now Stephanie, Margie, Brian, and Georgios, in that order.

STEPHANIE PERRIN: I'm actually responding to Thomas' proposal/suggestion/query here. I, too, have a dream. Brace yourself, Margie. It's binding corporate rules. I think honestly, as I said, we're going from 0 to 150 here. It's going to take years for us to harmonize our mechanism. So I don't think we're ready to come up with a code of conduct that is ready. It'll take us a while of implementation to get agreement on the parameters. But I certainly would think that would solve some of our problems. Then you would have an oversight committee keeping an eye on the code of conduct.

But don't neglect the possibility of binding corporate rules as well because, really, you want a mechanism to control the bad actors, and I'm not sure what it is. I leave it to you, contracted parties, to figure out how you're going to control the bad actors. De-accreditation by a quick and fair method would something that you would want to work on in your model. I'm not sure you're going to do that overnight. I think it's going to take years.

So I think we maybe ought to map out a --- big sigh; as I said to Thomas this morning, I intend to be in my rocking chair by the end of this – ten-year plan for what is reasonable to achieve, given how long this fight has gone on. That's a useful output when you put this out for public comment, lest people get all crazy like they have recently on a certain other topic that I won't bring up again.

JANIS KARLKLINS: Thank you, Stephanie. Margie?

MARGIE MILAM: I think the concept of actually working on code of conduct for this is interesting. I know you've been talking about this for a while, and I think it does what you want for the corporate binding without actually calling it that. I note that, on the ICO website, they've got a lot of information on how to submit a code of conduct. So there's been a lot of evolution now in this thinking over the last, say, year-and-a-half. So that might be a useful way to take this concept forward.

JANIS KARLKLINS: Thank you, Margie. Brian, followed by Georgios.

BRIAN KING: Thanks, Janis. I think the code of conduct idea is a good one. We could have a policy recommendation that instructs ICANN to explore that. I would just note as a word of caution that we're a couple years into GDPR now. I don't think there are any code of conducts approved yet by the Data Protection Board. I know that's a favored thing. As I understand from Brussels, the DPAs would like more codes of conduct to be submitted for review.

A word of caution. We're a couple years in and there are none. Our council says that it's probably going to take quite some time to go through all the steps to get a code of conduct approved.

So we need a policy that works now and while we work towards a code of conduct. So let's not forget that this has to work without … We can't put all our eggs in that basket, but that's a good thing to explore.

JANIS KARLKLINS: Thank you. Georgios?

GEORGIOS TSELENTIS: I think we said in the beginning that the perfect is the enemy of the good. In this sense, I think the code of conduct is something good to pursue. It's good to solve problems that cannot be solved with the contractual obligations that are currently in the contract. So it's something that we should put in our readout that we need to

develop. I think the question initially here was whether this group can contribute to this by updating and overseeing the code of conduct.

It's also true – what was said – that, although the DPAs have this inside the GDPR and they want to see more codes of conduct, we don't have evidence of something like this working now. That doesn't prevent us from putting the whole thing in motion and in place and foreseeing how, with our policies, this will play out.

JANIS KARLKLINS: Thank you. I have now James in line.

JAMES BLADEL: Just briefly, I think that the code of conduct idea is interesting. I don't want to hose it, but I should point out two points of caution. One is I think that code of conduct is a term of art under GDPR that's different than the way we defined it under the RAA. Maybe they're compatible. I don't know. We should look at that before we jump into this with both feet.

The second one is, if we don't have a way for the code of conduct to be dynamic and periodically reviewed and amended, then we've lost what we were trying to achieve originally, which is to not carve this stuff into stone and to allow it to continue to improve and evolve. So the code of conduct, if that's the mechanism we choose, has to improve and evolve as well. So it's a way of making it enforceable but it doesn't address our situation of how does it become dynamic.

JANIS KARLKLINS: Okay. Thomas?

THOMAS RICKERT: Maybe I should introduce this differently, but I was on the same panel with the previous Article 29 group chair and the former German federal data protection officer. We were discussing the question of codes of conduct. He explained to the audience what the beauty of a code of conduct would be, and I said that I see an additional benefit, and that is getting legal certainty on edge cases, something which is not really clear in the GDPR. He invited agreement that that would be a benefit.

I think that exactly the question of putting some dynamic into this process … I think we all know that this is a rapidly changing environment and that we might have more and different challenges in the years to come. Building that into a draft code of conduct to say how we're dealing with changes, how we are amending our decision-making practice, based on the intake from decisions and court cases and all that I guess is something that we will the find out whether the authorities are okay with. So we could get legal certainty on the dynamics.

So I think that, while everything that's true is true, it's a cumbersome process. It will likely take long. It's not built to be dynamic. I still think it's worth the effort because this entire industry is afraid of getting a big blow if somebody tells us, after we've implemented all this, that it's not possible and that we're completely on the wrong thing.

I think that even showing to the authorities, if we're putting effort into writing this and presenting it to them, will benefit everybody who might be involved in supervisory cases because they are looking at the track record that you have. So far, the track record is not particularly splendid, to put it mildly.

So I think we should really build that into it. The proposal to make it a policy recommendation, to draft a code of conduct, I think is an excellent one. So let's try to pursue that.

JANIS KARLKLINS: Of course, that is up to the team to decide on: if we can do it. But just let me argue. The idea that I heard was to ask ICANN staff to write the code of conduct. The question is, can they? Do they have enough operational experience in this area, especially if they will not run the SSAD disclosure decision-making process but the contracted parties will do so? Again, it's just a question.

Or we should think that this advisory group, if created, could, based on the analysis of operations of SSAD and exchanges of experience of different operators, whether it's a central gateway or at the contracted party level, collects enough evidence that they start drafting this code of conduct, based on experience analyzing the work of SSAD, and the present this code of conduct for consideration, or whatever procedures would be put in place. Again, I'm just asking questions.

I have Stephanie, if that's a new hand, followed by Marc and then Brian.

STEPHANIE PERRIN: Yes. Following up, I think this is definitely something that we should be thinking of long-term. If it is a recommendation, then we can build it as we go along with this oversight committee. But, at the moment, we don't have enough clarity, and the DPAs keep saying this about what we're actually doing. You can't go with a vague code of conduct to the DPAs and get it accepted. I'm old enough to remember when the direct marketers in Europe were busy working on theirs. It took blessed decades.

Now, I think we would have a stronger impetus here to get the darn thing done, maybe even five years. Who knows? But, right now, we can't even tell the DPAs clearly who's controlling what and where the agreements are and what the division of accountability is. So forget it. We've got a lot of work to do before we get to the code drafting stage. Thanks.

JANIS KARLKLINS: Thank you. Marc?

MARC ANDERSON: Thanks, Janis. I think the code of conduct is an interesting concept. From around the table, you see there's definitely interest in us talking about it some more. But I think we maybe we got off target a little bit. I don't think talking about a code of conduct is critical for getting the draft report out. So maybe this could be a topic that gets sent off to Work Stream 2 items to talk about after. I don't think we need to talk more about code of conduct here in terms of getting our initial report out.

JANIS KARLKLINS: Thank you. The last is Brian.

BRIAN KING: I'm going to strategically raise my hand after Marc every time because I agree with everything that he said there. Let's do it that way. Let's put it there. And I was going to suggest that we move onto the rest of the agenda because, as you said, we have to get the report out. Thanks.

JANIS KARLKLINS: Thank you. So thank you very much for input. I think we have something to reflect on and should propose to the advisory committee the idea in writing. I still maintain my call to team members for when they want to come to the board and think and add some functions that this advisory group could do or edit what is on the board. New pens have arrived, so it will be more visible. We would try to summarize and then put it on paper for our consideration maybe tomorrow as a part of the overall mechanism because this part of the overall evolutionary SSAD mechanism that we're working on which has a direct relevance to the initial report.

With this, I would like now to go to the GAC and see whether we could accept what the GAC is proposing in terms of accreditation of public authorities to operate or to use SSAD. So the GAC sent us a proposal, and I would invite Chris to maybe highlight the most important elements of that proposal before I open the floor for an exchange of views. Chris, please go ahead.

CHRIS LEWIS-EVANS: Thanks, Janis. We had a discussion about releasing what we released or to tie it down to what wouldn't need to be in the initial report. We thought it's just helpful to give you exactly what we gave to the GAC members. As hopefully you can recognize some great copy and pasting of Alex's work – thank you very much to Alex, certainly around definitions and everything else; I thought I'd better to say thank you to Alex before being accused of plagiarizing most of his good work – some of the important points are eligibility. We've got a small list there. This is not everyone.

The idea behind this is to just get some of the GAC members onboard with the sort of bodies we're talking about. When we're talking about a country deciding on who would be eligible for accreditation, it's very much focused around parties that have a public task to request some of the status. So we're not looking to lump everyone into this. It's really around a fine definition [for] people with public policy tasks to actually look for some of the data requested [later].

So I think that's the main one. There is a lot borrowed from our accreditation principles for non-governmental people. We still have de-accreditation there, which I think is very important. Quite some discussions went on around that, as you can imagine. That's just because, if they get accreditation, it doesn't mean you can get data. The Contracted Parties House, where now the model has gone to, still have that right to say no. It's an almost automatic accreditation. It's not an automatic disclosure of data. So it's very important that the safeguards that we've talked about – I know Georgios has mentioned some of those before – all apply. All the decision-making process around the reason to

disclose still applies. This is just around getting an organization or authority the ability to ask for that data.

Log-in is in there. It's all very important. We talked about transparency reports and things like that. So I think that has been included in here. I know it's in our public one as well. For me, it's very important that that is available, obviously not straightway after every single request. But, again, it will be whatever the reporting structure is on that.

Other than that, I don't really want to go through it bit by bit, so I'm happy to answer any questions or get Georgios to. Thank you.

JANIS KARLKLINS: Thank you, Chris. I think the important element is that each country or territory will define or designate an accreditation authority. This accreditation authority will organize the process of accreditation of all public entities that will want to work with or use SSAD. Among those local authorities would be law enforcement authorities, judicial authorities, consumer rights authorities, cybersecurity authorities, including [inaudible], and data protection authorities. So that is defined.

This accreditation authority probably is only the missing element in the description that you provided. The national accreditation authority will need to have some kind of formal relationship with an SSAD accreditation authority. In other words, ICANN org or an outsourced organization will act as the accreditation authority on behalf of ICANN org have interoperability, and that interoperability would be also somehow documented.

For the rest, of course, I would say, if your proposal is agreed to by the team, we would take your copy/paste things out because there is no point in having two similar accreditation bits in the initial report. But we would put it as a separate sub-chapter in the accreditation chapter, clearly describing the functionalities of national accreditation authorities, including also de-accreditation.

Are you in agreement with me?

CHRIS LEWIS-EVANS: Yeah. Thanks. Just to quickly respond to that, I totally agree with that. I think, when I initially wrote this, which was quite some time ago now, we hadn't agreed on the public accreditation – what was in there, what was not in there – so, as I said, this was given to give the GAC a full briefing. So I think, rightly so, we can strip bits out and put it as a sub process. That would be agreeable to us. Thank you.

JANIS KARLKLINS: Thank you, Chris. I have Alan Woods followed by Marc Anderson.

ALAN WOODS: Apparently the registries are ganging up on you. Sorry.

CHRIS LEWIS-EVANS: I'm used to it.

ALAN WOODS: Ouch. So thank you, obviously, for this. There's one thing which I think is important that I didn't see when I was reading through this. I think it's an advice more than anything. We need to be obviously be very careful. We need to delineate more the concept of [more of] the official authority to get this information. Yes, we talked about this in the past as well, where there are specific legal powers, specific legal requests, that you can make for – you know yourself – the investigatory powers and things like that. You don't talk about that in the process of accreditation. Those people in the accreditation should ensure that they say "In certain instances, we have an actual statutory or jurisdictional power to take this." I think that would be very helpful to have that in the accreditation as well. Under what power would I have been exercising this right in your own accreditation process? Because that makes the 61F on our basis a lot easier because, if you're exercising a right that is good and proper in a proper exercise of the powers that are given to you as LEA or even to anyone of these bodies, it would be a lot easier and a much more straightforward 61F consideration in our mind. So it'd be very important to have that as part of parcel of the accreditation because the onus is not on us to understand why you're asking but on you to provide to the controller why you are asking for that or under what powers you're taking that.

So that was maybe up the level of officialdom, almost, in it because I think that's an opportunity that was slightly missed in this.

The second point is on the confidentiality point with regards to the logging. Again, it goes back to the onus on that one. I think it's very important and we haven't really mentioned in anything that

we've drafted yet. We need to be sure that, if you have an expectation of confidentiality, that is then communicated. We can't just assume that is confidential because confidentiality is not something that applies to us unless we are told is an obligation on us. So I just want to make sure that that's in there as well. Thank you.

JANIS KARLKLINS: Thank you. Marc, please?

MARC ANDERSON: Thanks. I had similar questions about how you saw confidentiality fitting into this. Alan made some good points, so I won't duplicate them here.

I wanted to point out – this is maybe more for how what Chris provided gets incorporated into the draft SSAD model – that really what you've defined is written as accreditation but is almost the role of an identity provider for a very specific purpose – for government officials or government organizations. So, when this is being incorporated, I think it maybe fits in the category of identity provider for this very specific use case.

A couple questions for Chris. First, as I was looking through this, I wanted to get a little bit of your take of how you see accreditation of entities versus individuals. I'll just the FBI as an example. How do you see one accreditation for the FBI and then anybody authorized to the FBI to use that credential would have access to it versus individuals at the FBI being able to request individual credentials?

That rolls into my next question as to how that plays into the oversight role. What kind of monitoring and oversight would occur to address bad actors? Because I think that varies quite a bit if you have a one-to-one requester to credential relationship versus maybe a shared organizational-type credential.

So I was just hoping to put you on the spot a little bit to expand on that. You're welcome. Thank you.

JANIS KARLKLINS: Maybe I will collect further inputs before giving the opportunity to Chris to expand on the thinking.

Stephanie, please?

STEPHANIE PERRIN: Thanks. At a quick-glance refresher on that document, I don't see anything on transborder requests, so how would you handle an accredited … It gets particularly difficult when it's an administrative investigation. In Canada, we have an agency that is accountable federally for protected species, whether it's whales or polar bear parts, and they will want to investigate the countries that are selling our black bear hearts. How are you going to deal with that?

JANIS KARLKLINS: Okay. So the next question comes from James.

JAMES BLADEL: Sorry. I got up to stretch my legs. I just wanted to answer one of Marc Anderson's questions because we've built an LEA portal for use by the U.S. DOJ. It becomes a clearinghouse for U.S. law enforcement, and we're working with Interpol to do the same for folks outside the U.S.

To your question of individuals versus agencies, the way we address that is that, at least in the latest iteration saw, is that everyone who is using that is using it on behalf of their agency. Otherwise, they wouldn't be permitted to use that portal. That was actually a sticking point during the negotiations because a lot of folks were saying, "Well, how do I control for all of the different officers?" The answer was that they had their own internal policies governing how those resources are used. It's the same way why people can't use the police cars' onboard computer, for example, to look up politicians and celebrities and things like that: they're bound by certain internal policies. So it is a little bit of a leap of fait that they have those internal controls in place, but it was good enough to let us address that question. So it's doable.

I don't know. Chris, is that aligned with your memory of that?

JANIS KARLKLINS: Chris, please?

CHRIS LEWIS-EVANS: I'll go for that one first that James has teed up nicely for me. Realistically obviously we've got many different countries that we've got to consider and different agencies. As you mentioned the FBI, they have 400,000 different law enforcement agencies in

the U.S., or that's what it seems like, I think. So, as James said, you have to get that agency to agree to only allow probably employed people with [inaudible] – sorry?

UNIDENTIFIED MALE: Authorized.

CHRIS LEWIS-EVANS: Authorized, yeah. So we're not talking about contractors or someone who comes in [off the street] and can use a system just because they want to make a WHOIS request and, "Oh, look. You're already authorized." So all that is well-documented. As you can quite believe, many of these types of organizations have to log and document everything. Are we going to stop 100% of the bad actors? No. In a similar way that the contracted parties can't say that they can stop actors, it's a fact of life. But I think, if we do the log-in principles that we can put in place, we'll be there to be able to find that person. As for any de-accreditation, if it's a one-off and it's a person, we can kick them off. There will be definitely in this world ramifications for that single person with gross misconduct type issues and everything else – normal employment [side.]

So I think that's fairly easily covered, hopefully. Realistically, that agreement will be shared. I think, as James has indicated, there's agreements there that can be held up as examples of how this may work.

Coming to the lawful basis thing, I tried to get this as high-level as possible really and not say all the different elements that'll be

collected around what purpose you're collecting for and if it's covered by a lawful basis and how you would do it in your country if you were going to serve. If that's something that will help automatization of a request, then, yeah, guess what? That's getting included. So, for me, that's more of an implementation thing, that that is one of the things that you need to put in to help with that decision-making process. I think I did put [it in] somewhere. Sorry if I'm not [inaudible]. Certain elements will be required to be submitted per request. That's more on that request side.

I'll go for your bear example. They will be accredited. They are making a 61F request if it's outside of the country, the same as anyone else. It's up to the contracted parties to decide whether they have that lawful basis. And it's a [great] purpose. So they might get the data. They might not. It's all dependent on that balancing test, [which] needs to go ahead. As Alan has said, it's based upon the different aspects and as much data as we can give them to make that test. If you can say, "Well, we are a federal agency and we protect [endangered] species," that's going in there and that's going to make his decision a lot easier to make. Obviously, we would prefer this to be as automated as possible, but guess what? [inaudible] six months, he says hopefully, to three years. That's what we're going to have to live with. Is it better than what we've got now? Yes, definitely. That's the whole reason for trying to push down where we're going. It's going to be better than it is now. I do have rose-tinted glasses on. Soon it's going to be even better.

STEPHANIE PERRIN: Can I do a follow-up on this? Thank you for that explanation. We had a little discussion this morning about reputational learning in an automated system. It will be useful to know how often requests are being turned down legitimately or illegitimately. Similarly, it's useful to know how often sloppily-put-together requests are being put in so that, if the system could create stats that the oversight committee could review, it would help us. And it would also help us create that code of conduct that Thomas is talking about because then we would have some idea of the vectors that we need to keep an eye on for a proper, clean system. Thanks.

JANIS KARLKLINS: Okay. I understand that there is no major difficulties with the suggested accreditation model of public authorities. Also I understand that you are fine adding that there should be agreement or at least a notification mechanism between the national accreditation authorities and ICANN org as the accreditation authority of SSAD and then an exchange of information and operations. And you do not have any difficulty with the request that was made that the confidentiality requirement needs to be clearly stated when the actual request is submitted in the system. That would indicate the course of action by disclosers.

So – yes, Chris?

CHRIS LEWIS-EVANS: Sorry. Very quick. Just to respond to that, I think [I'd like to make it clear]. I think I would like to tie that down a little bit to make some people feel maybe a little bit easier about that, around where it

would have a negative impact onto an investigation. It's not necessarily for everyone. It's where the least of that information would majorly an investigation. So we're not talking about that all government bodies get the right to submit a confidentiality request. It would be limited to those carrying out some form of investigation, which obviously won't apply to every single one of the [ones] accredited by a government.

JANIS KARLKLINS: Yeah, but that does not change the requirement of explicitly saying that this should be kept confidential for whatever reason.

CHRIS LEWIS-EVANS: Yeah.

JANIS KARLKLINS: Okay. So then we're done with this. We will add – yeah/no?

UNIDENTIFIED MALE: [inaudible]

JANIS KARLKLINS: No. Alan's hand is new and then – no, Alan G's hand is new.

ALAN GREENBERG: Thank you. Just a very quick question. Once we settle on all of this, how do we propagate it to countries outside of the GAC?

CHRIS LEWIS-EVANS: We will probably use something like Interpol as a way of spreading that out because they're already aware of the WHOIS issue and obviously they have a wide number of countries who are members.

JANIS KARLKLINS: Okay. Alan Woods?

ALAN WOODS: Thank you—

CHRIS LEWIS-EVANS: Sorry. And I would ask our Contracted Parties House friends also to make it clear that, if you're a government, there's a way of getting access to it.

ALAN WOODS: That's a good point. Just going back to your point there about the confidentiality, I suppose my only – worry is too strong, but obviously we have data subject rights that we need to look after. One of the data subject rights is obviously the right to access, the right to know who has received the data. So it is a competing right, and there are certain provisions with the GDPR that we can use to say, "Hey, I'm not going to actually give you access to that particular data or tell you who I've released that to." So we would need something like that to prevent us from not releasing where we asked. So it's a consideration. I think it is important. If you want

to have that confidentiality, I fully understand why you would need it. But it does need to be almost formally established to prevent us from releasing it as well.

JANIS KARLKLINS: Thank you. So then we're done with this part. We can now go to the list of issues to be clarified. The staff sent out this list to the team yesterday. My idea would be to let staff introduce, let's say, a bigger chunk or a step by step. We will start with accreditation. Then we would let groups discuss among themselves and we'd come back with a possible agreement on the suggestions that staff is proposing in the table.

Maybe now would be the time to distribute that paper to each group simply for ease of reference. So we will go step by step, issue by issue, during the remaining time today and tomorrow.

I also forgot to say please do not plan any dinners tomorrow. We may need all the time at our hands while we're present in Los Angeles to work through the outstanding issues. So, if we will swiftly continue and go through the topics and make necessary agreements, we will end up as suggested at 5:30. But, if we will have a feeling or I will have a feeling that we'll need more time, then we will stay tomorrow as long as we need in this nice room. We'll use the [U.N.] method to work throughout the night. And that's not a joke. I'm using now my Chair's prerogative to warn you.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: Me, too.

THOMAS RICKERT: Consensus by exhaustion, right?

JANIS KARLKLINS: So this is one of then methods, yes. I hope we will not need to stay after 5:30 tomorrow, but, just in case, be aware.

Yes, Marc?

MARC ANDERSON: Quick question, Janis. The issues list and the proposed edits we should be reviewing against the Chameleon draft?

MARIKA KONINGS: Basically you have to look at, in the first column, the issue as it was on the original list because it's a very long document with many comments related to the model. So we've taken all those out because those are being dealt with separately. In the second column, you see the comment and by whom it was made. But what you see in the third column is what you need to look at. It's the proposed rewording based on that comment. We haven't applied that change yet in the Chameleon model document because we want to wait for this conversation.

So, from a staff perspective, apart from a couple where we said whoever made the comment should maybe provide specific suggestions to what they proposed, many of these seem more as clarification and minor edits. But, again, we think it's important for then group to review those and then walk through those and then flag which of these your group cannot live for inclusion in the initial report.

To facilitate your reviews of the document, there are also a number of items that are highlighted in blue. Those are items where a group made a comment, but either it's one that was already previously discussed and agreed on and doesn't seem to be new information that would warrant that change or it was already addressed somewhere else. So we tried to explain that at least we're suggesting that no change is needed, although we have put in the current language, so you can actually see what is currently there. But, if there's no bold language, it means that at least staff leadership are not recommending any changes at this point in time.

I hope that explains it.

MARC ANDERSON: Thank you. That helps. So this list was derived initially from the feedback given on the previous draft, right?

MARIKA KONINGS: Yes, but it's on those aspects that have not changed as a result of the Chameleon model.

MARC ANDERSON: Okay. But the goal posts have moved a little bit, so we have to keep that in mind as we're reviewing this, right?

MARIKA KONINGS: Yeah. I think, if remember well, in those where we did make changes, we did make changes. We updated the language because, of course, in the Chameleon, the main thing was, in a number of the recommendations, specify who would be doing what. So I think that you will already see in the language that's posted here. If there were changes in that regard, those should have been applied. But, as I said, most of these don't relate or shouldn't relate to the kind of model discussion but really more to other aspects that either have been discussed before or where people have flagged, "I have clarifying language that I think should be added," or clarifying questions. In some cases as well, there's a restating of, I think, previous positions made. This is where we suggested we've gone through that and maybe let's not reopen it. So I think that's really to ask for the group as well.

For this first block, we suggest cutting it into groups so you don't spend two or three hours going through it. So, for the first one, the proposal is to look at the accreditation comments. So it says the first block in the document. Again, the ask is really look through that with your group. As I said, several of these here are clarifications. A couple of those are where we said there's probably no need to change that because either it's probably previously discussed or agreed upon or it's already clarified in another part of the recommendation and basically come back to

the group only flagging those issues that you cannot live with the way it's proposed to be dealt with. So I think we want to avoid going one by one. I don't know how Janis wants to manage it, but it's probably [going around] and saying just name the numbers of the issues that you think your group cannot live with as is proposed. I think then we can make an assessment of how to best deal with those or have groups as well state what is the issue that you cannot live with and what would need to change for you to be comfortable with the language for inclusion in the initial report and, as Janis noted before as well, factoring in the positions from other groups made on those points.

I hope that helps.

JANIS KARLKLINS: Basically, please look at the comments in the second column and look at the third column, the proposed rewording, and see whether you can agree with the proposed rewording or you can live with the proposed rewording in each of those boxes. So, in the blue, you can see the comments which are suggested which clarify the middle column. The Y in the middle column is suggesting to keep the existing wording or so on. So, basically, your task would be to review the second column against the comments made by different groups in the first column on accreditation-related issues. We will come back in, what, 15 minutes? 20 minutes? How much time do you think you need? It's not an overly difficult task. Maybe let's opt for 15 minutes, until 2:30. Then we have time to go through those issues quickly and—

MARIKA KONINGS: Just accreditation.

JANIS KARLKLINS: Yeah. Just accreditation. Nothing more, which means that this is the first four pages. Okay? 15 minutes. Please come back with the positive answers.

I hope you had a chance to review the comments and proposed rewording on the accreditation building block. The method that I would like to propose is the following. Initially, I would ask all groups to name the number of the issue that you have a problem with.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARLKLINS: Yeah, that you cannot love with. Just give a number. We will see if there is any more problematic issues than others. Then we will address those problematic issues one by one.

Brian, what's your number?

BRIAN KING: Thanks, Janis. It is 24. I think – yeah. 24. I think we would disagree with the—

JANIS KARLKLINS: Wait. Just 24. That's enough for the moment.

Chris?

CHRIS LEWIS-EVANS: 0.

JANIS KARLKLINS: Alan?

ALAN WOODS: [inaudible]

UNIDENTIFIED FEMALE: Microphone.

ALAN WOODS: Oh, sorry. Not to a huge extent, but we kind of agree on 24. It is probably not correct.

JANIS KARLKLINS: 24? Okay. Thomas?

THOMAS RICKERT: 27.

JANIS KARLKLINS: Please, again?

THOMAS RICKERT: 27.

JANIS KARLKLINS: 27.

UNIDENTIFIED MALE: Add one more for 24.

JANIS KARLKLINS: 24. So then we have a problem with 24. 27? Anyone else?

UNIDENTIFIED MALE: [Volker]?

[VOLKER GREIMANN]: I was going to say 0, but I like the change in 27. So making it more neutral is good.

JANIS KARLKLINS: Okay. 27 we will discuss. Alan?

ALAN GREENBERG: I'm not sure. When people are saying that they have trouble with, for instance, 24, is it having trouble with what the comment is or what the change is? So I'm not quite sure exactly what people are having trouble with. I'll add my name to 24 also, but I'm not sure I'm agreeing with the others.

JANIS KARLKLINS: Okay. So we need to discuss 24 and 27?

Brian?

BRIAN KING: And 25 also, please.

JANIS KARLKLINS: 25 as well. Okay. So then I take it that as, for the rest, we can live with the proposed wording in this table.

Now let's—

UNIDENTIFIED FEMALE: [inaudible] 24 [inaudible].

JANIS KARLKLINS: Yeah. So now I'm asking Marika to walk through 24, 25, and 27, please.

MARIKA KONINGS: One by one, or you want to do a [inaudible].

JANIS KARLKLINS: One by one.

MARIKA KONINGS: The first one on 24: The language that is in the current report says that both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity warrants that the individual is asking on the authority of the accredited entity. This is a reminder that we put in the comments. This is actually something that the group discussed and agreed on during the Montreal meeting. That comment that was provided was from the NCSG, noting, "Shouldn't this be reversed? The accredited entity must warrant that the individual using its credentials are acting on its authority? The accredited entity can be held accountable for the individual's actions." So the proposal by the NCSG was basically swapping that around.

As I said, staff felt hesitant to make that change because that was something that was originally agreed on and discussed, but it seems that a number of groups – again, to Alan's points – are not agreeing with the staff recommendation of not touching it at this point but are agreeing with the proposed change. So maybe we just need to get clear from those who flagged this. I had the IPC, NCSG, the Registry Stakeholder Group, and ALAC flagging this one as that they could not live with what staff has proposed, which is not touching this – oh. Registries are off? Okay. So it may be worth for the group explaining why they cannot live with the staff proposal to not change this language which was previously agreed on by the group.

JANIS KARLKLINS: Thank you, Marika. Brian?

BRIAN KING: Thanks for clarifying, Marika. In that case, we withdraw our objection, too.

JANIS KARLKLINS: I have three hands up. Chris?

UNIDENTIFIED FEMALE: That's an old hand.

JANIS KARLKLINS: Alan G, your hand is up. Not any longer. Yes?

MARIKA KONINGS: Volker [inaudible]

JANIS KARLKLINS: Volker, your hand is up? No?

MARIKA KONINGS: It's an old one.

JANIS KARLKLINS: Okay. Stephanie then? Stephanie?

STEPHANIE PERRIN: I think our objection to this is that we really think it's been flipped around. Can you give me an example of an accredited individual that is not backed up by an entity who would be entitled to use the system?

Part of the problem was the experience we went through in the RDS, where we had crimefighters self-educating themselves in their basement, claiming to be saving the Internet. I'd like to see those guy accredited. I don't mind accrediting an entity even if that entity is one individual. But they would have to go the same thing that an organization entity would go through. It is not clear what's happening here.

JANIS KARLKLINS: Brian, please? Let's use Zoom rather than raising hands, okay? Alan G?

ALAN GREENBERG: I think the problem is that both directions are true. When an entity is accredited – an entity – it warrants that it will only give out its accreditation information to people who are duly representing it. When the person submits the specific request, it warrants that it is representing the organization. So one is a warrant in advance, saying, "I'm going to use it that way," and the other one is, when the specific thing is submitted, goes in the other direction. So both of them true, depending on what timeframe you're looking at.

JANIS KARLKLINS: I recall this conversation that we had in Montreal on this topic. It specifically mentioned that, if the organization is, let's say, small or medium-sized, they may choose to get accreditation for the organization, and everyone who would file the request using credentials of that accredited organizations would act on behalf of that organization.

But there might be a big organization spread across the world. They may choose to accredit or get a number of accreditations at different parts of the organization. I'm looking to Microsoft being one of them, potentially where one organization would have four, five, six, or seven accreditations. But then the officers of each branch would use specific credentials of that specific branch to conduct their business. That is reflected in the language that we agreed on in Montreal. As Alan said, it goes basically both ways. It's a chicken and egg problem.

Laureen and then Brian.

LAUREEN KAPIN: I think Alan's comment was very helpful. I think Stephanie's point is not to say that she disagrees with the concept of an individual warranting that they're acting on behalf of the organization. What I'm hearing Stephanie say is that it needs to be clear that that first premise that Alan identified has been fulfilled – i.e., in advance, the organization warrants that everyone acting pursuant to this authorization is in fact what they purport to be. Yes? So I think it's a clarity issue. I actually don't think it's a substantive issue.

For example, the FTC had a portal and a system for making a request. The only way, practically speaking, I would be able to access that portal is through whatever link or place in our Internet made it possible. So, in practical sense, I wouldn't even be able to get in the door unless I had the keys to the door.

But I'm hearing Stephanie say she wants some clarity, not that she is disagreeing with the individual warranting that they're acting on behalf of the entity.

STEPHANIE PERRIN: If I may do the follow-up on that, that's exactly my problem. I do recall the discussion, and I pointed out that one of the biggest problems is revocation of credentials. And you don't know how a system is running. Similarly, in our government – well, I could tell you stories. But it is relatively trivial to make sure that that individual credential operating for an accredited entity is time- and date-stamped as it goes out the door and you know it's valid and somebody is vouching for it. Otherwise, you're looking at a bigger audit load, and we're trying to cut costs here.

So, since inevitably we are going to have to audit those accredited entities, let's try to keep the cost down by insisting that the entity has some meaningful attribute pinned to that request as it comes in. Does that make sense?

JANIS KARLKLINS: We were talking exactly that each entity will have internal policy, or key, as you called it, Laureen, that ensures that every officer of that entity would act according to policy and would perform

functions according to standards set by the organization itself. We are at the point where we need to, if there is a disagreement, to please come up with concrete language. If there's no concrete-language proposal, we can talk in principle until tomorrow morning, only on this point. But I do not want to do that.

So, Stephanie, do you have any specific language that you want to see reflected in the second column?

STEPHANIE PERRIN: I think my concerns would be washed if the accredited entity signs the request.

JANIS KARLKLINS: How do you see that in practical terms? The entity is abstract. It's a legal construct. The individual is the one who will sign off on behalf of the entity. According to the entity's policy, this individual will be authorized for acting on behalf of that entity.

STEPHANIE PERRIN: I really hate to slow us down here. As I say, revoking credentials is one of the hard jobs. If you just have a staff list of people or contractors who are eligible to submit requests, then you are relying on security to revoke those credentials.

If, on the other hand, you have tokens that are issued from the entity, and those tokens are date-limited … I'm way out on a very slim limb here because I'm not a geek; I'm a policy person that has beaten up the geeks for not having proper controls in place.

So this may be totally outdated, and I depend on our technical people like Martin. He's not listening, so he can't help me out here. I want a signature that's date- and time-limited so that somebody doesn't show up using a credential that was authorized while they were under contract to – I don't know – Apple, say, six months before because, if you say the company shall have policies and procedures, then you're on the hook to go in and audit them. That's extremely expensive, and we're never going to have the money.

JANIS KARLKLINS: I think it's a far-stretched concern. My sense is that we need to leave the language as is. It reflects also including what Stephanie is arguing. We may take a note for implementation, some kinds of points suggesting that an accredited organization should develop internal procedures or something of that sort.

Would that be acceptable?

Alan?

ALAN GREENBERG: I think the answer is in the implementation note. The whole concept of having an accreditation for an organization which is then redistributed – we're going to have to make sure that someone can attribute it to the actual person who did it. Date- and time-stamped is a good thing. So I think, when we come to figuring out exactly how we issue credentials to organizations and how they enter who they are on the request is something that we're going to have to, to be blunt, make sure we have security

professionals looking at and make sure it's done properly. I'm sure we could talk for hours about good ways of doing it. It's not our job. We're not the experts. Let's have an implementation note saying individuals using it on behalf of larger entities are going to have to have some careful procedures. Thank you.

JANIS KARLKLINS: With that, we move to Item 27.

MARIKA KONINGS: 25.

JANIS KARLKLINS: Oh. 25.

MARIKA KONINGS: I think 25 was flagged by the IPC. This deals with a section in the accreditation language that says, "Assertions as to the purpose(s) of the request" … And a comment here was made by the ALAC: "Each request should have one purpose. Data sets disclosed vary depending on the purpose, and it's important to be able to track the data disclosed to [the requester] [inaudible] certain purpose. In addition, different purposes have different legal bases and different rights to the data subjects associated with it."

Staff here also noted that this was a topic that has been discussed on numerous occasions. It was previously agreed that a request may have multiple purposes associated with it. As such, we were

recommending not to make any changes to this. But I think the IPC has concerns about that.

UNIDENTIFIED MALE: Thanks, Marika. I don't have a concern about leaving it as is because it's the way that we wanted it. But I do think – I don't want to speak for Hadia, but we were chatting about this, too – that ALAC had a valid concern that, especially in an automated scenario, it would be tough to automate if there are different purposes and, at the same time, that warranted different data to be returned. But I think a technical solution is probably a better solution than a policy one on that. I would think that we could probably all still agree to the language that we had before about multiple purposes per request from some concerns the NCSG had. Thanks.

JANIS KARLKLINS: But, again, it's not so difficult to technically implement multiple purpose indications. Instead of single notifications, you can have two or three points which indicate what our purpose is for the specific request. That goes in the system with multiple purposes, so it's not all that difficult to implement. So we'll leave that as is.

27 now.

MARIKA KONINGS: 27. That comment was made in relation to Point H. It defines a baseline code of conduct that establishes a set of rules and contributes to the proper application of data protection laws,

including the GDPR, for the ICANN community, including …" The comment was specifically attached to the reference to GDPR. It's a very long comment, so I won't read it all. Thomas can speak to it when he gets the mic. But I think the gist was that the report should be specific that these recommendations are made in response to GDPR. I think he referenced various parts in the report.

Our suggestion here was it seemed to be a general comment and maybe not specifically to this sections. So it may be worth if the ISPCP wants to put forward specific language to convey that point in the report so the group can actually see that. I guess it would more be part of the introductory language to the recommendations. That was at least our suggestion.

JANIS KARLKLINS: Thomas?

THOMAS RICKERT: I did not offer concrete language because I think that this is a general topic that our group needs to decide because you'll find various places in the report where we are beating about the bush. On the one hand, we're explicitly coding parts of the GDPR, and then we say it's abstract and must be globally applicable, which is understandable because ICANN wants to be inclusive at the global level. But some of the statements might not even been true, that what we're establishing is in compliance with various other data protection laws. Chances are good that we're compliant with a lot of national laws because GDPR is quite a high bar.

What I would like to suggest is that, in the introductory part of the report, we would state that ICANN tries to be globally inclusive, allowing contracted parties to comply with applicable laws, and that the EPDP and the temp spec is a specific response to the GDPR and that, therefore, this report references GDPR but that this shall not take away from ICANN's aspiration to be inclusive at the global level. Something to that effect. If this group is okay with that, I can plow through the report and come up with suggestions to make that work.

JANIS KARLKLINS: Thank you. I hope, since this is a common-sense thinking, we may go that route. The question is whether we could do it as a, let's say, introductory statement prior all recommendations because they're relevant, basically, to all recommendations. Or we are putting it as a footnote in specific places where we're referring to GDPR concretely but also say that this may also apply to any other national legislation.

THOMAS RICKERT: If I may, Janis, I would strongly recommend that we have an explicit part in the introductory section of the report because we heard from individuals that they say, "Well, why are you doing this for the Europeans? Do you not take our local laws seriously?" Therefore, I think it warrants an explicit statement in the report to explain why we're doing what we're doing.

JANIS KARLKLINS: I have Alan G and then Stephanie. Alan G, your hand is up.

ALAN GREENBERG: Thank you. I think we should take Thomas' offer to go through the document and find all the places and draft something to begin with and run quickly before he changes his mind. We've waffled back and forth many times about, "Well, this is not just GDPR. We should be specific about appropriate privacy legislation," and then we scatter 61F all over the place, which is about as specific as one could get to GDPR.

So I think that we should say, "This is GDPR," and not be ashamed of it and say, "But we believe and we aspire to be compliant with other local laws as well." Thank you.

JANIS KARLKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: I'd just like to the record to show that the Canadians are in remarkable agreement today. I agree with what Alan just said. I think we should jump on Thomas' offer.

I would suggest that, in that introductory section … I know there is reluctance to accept the GDPR as having set a global standard, but the GDPR does happen to be the only regional harmonized regulation. As such, it represents how many countries now?

UNIDENTIFIED MALE: End of the week?

STEPHANIE PERRIN: End of the week. Right.

JANIS KARLKLINS: Still 28.

STEPHANIE PERRIN: Right. And there's no other global standard that meets that. So I'm sure Thomas can come up with some delicate diplomatic language that addresses the fact that the standard is being set by Europe and that other laws may differ and each different instance of this in the port is going to be different because we have to insist that registrars continue to meet their own local laws, which can be wacky. Thanks.

JANIS KARLKLINS: Then I understand that Thomas is to draft one sentence for the introductory part of all recommendations, suggesting that these recommendations are drafted with the GDPR in mind but aspire to comply with all privacy legislation around the world. Something to that extent. So you have 45 minutes, Thomas, to draft the language. Thank you.

So now – yes, Alan?

ALAN GREENBERG: To be clear, he also said he'd go through the whole document and find places where we're saying the opposite. I think that's a necessary part of it, so 45 minutes might not be quite sufficient.

JANIS KARLKLINS: So you have an additional 15. Just joking.

Laureen? No? You took off your hand. Okay. Good.

Then we can go to the next set of questions. Those questions will be on the receipt of acknowledgement, response requirements, and acceptable use policy. The methodology is exactly the same. Marika will introduce all the issues. We will break for group talks and come back for conversation. Marika?

MARIKA KONINGS: Thanks, Janis. Basically, indeed, as you said, there's a number of different sections here that you asked to review. You'll note here that, in some cases, we're actually referring to other sections where things may be better addressed or are already being addressed -- for example, the first comment on 36. In some of these cases as well, specific language was suggested but staff has proposed alternative language, which we think may better address the issue. There's quite a few here as well where we, I think, basically discussed issues previously and did things for certain reasons. Or maybe questions.

Again, the question is, is any new information provided that would warrant that conversation? We didn't see that in the actual comment that was provided, but, of course, if the groups that have

provided those comments have additional information they want to provide on why certain issues should be reopened, I think that's something they may want to think about during the break as you look through this. Again, we really appreciated, I think, in the first review that you did that you really focused on those issues that you cannot live with, that raise to that level. Of course, if you come across any kind of minor changes or edits, you can take those directly to us.

So I think, with that, on to the next section. Oh, one administrative note here. I don't know if any groups went to the kitchen, but apparently that's off limits for visitors. But we do have – Terri, which office?

TERRI AGNEW: 312.

MARIKA KONINGS: 312. Where is it exactly?

TERRI AGNEW: It's right across the hall, one door down from the café. It's in the other hallway.

MARIKA KONINGS: Okay. So it's in the other hallway. 312 can be used for those groups that want to go there.

MARC ANDERSON: Which sections again, please?

JANIS KARLKLINS: These are the sections: receipt of acknowledgement, response requirements, and acceptable use policy. Pages 5 to 11.

Now it's 3:05. Let's say 3:25 to be back in the room.

TERRI AGNEW: Does anyone want to use 312? I can take you over there.

Okay.

JANIS KARLKLINS: So group conversation until 3:25.

THOMAS RICKERT: I have sent language for the introductory part to the mailing list. So maybe you can take a look at it. I'm plowing through the report to find other places where we need to do some [inaudible].

JANIS KARLKLINS: Thank you. I like that team members are following the Chair's instructions. Thank you.

So we don't have the IPC folks.

MARIKA KONINGS: [One of these we're] first collecting anyway.

JANIS KARLKLINS: Let us now collect the numbers. Like in the previous exercise, please indicate which numbers from the three sections – receipt of acknowledgement, response requirements, and acceptable use policy – you cannot live with, with the formulations in the middle section.

UNIDENITIFIED MALE: 36.

JANIS KARLKLINS: 36?

UNIDENTIFIED MALE: 36.

MARIKA KONINGS: Which one? 36?

JANIS KARLKLINS: 36.

UNIDENTIFIED MALE: 36 and 46.

JANIS KARLKLINS: And 46.

MARIKA KONINGS: And both registrars and registrars [inaudible]

UNIDENTIFIED MALE: Yeah.

UNIDENTIFIED MALE: Yeah.

JANIS KARLKLINS: Okay. Mark?

MARK SVACAREK: 36 and 45.

JANIS KARLKLINS: 36 and 45.

UNIDENTIFIED MALE: Same thing.

JANIS KARLKLINS: Same there. Stephanie?

STEPHANIE PERRIN: 46 and 56.

JANIS KARLKLINS: 46 and 56. Okay.

JANIS KARLKLINS: [inaudible]?

UNIDENTIFIED MALE: 53.

JANIS KARLKLINS: 33?

UNIDENTIFIED MALE: 53.

JANIS KARLKLINS: 53. Okay, that's it. So we have 36, 45, 46, 53, and 56. Then I take that as, with the rest, we can live with them. Okay, good.

Let us now then go to 36. As it was the case, Marika will kickstart the conversation. 36.

MARIKA KONINGS: Starting with #36, the language that is currently in the report in relation to receipt of acknowledgement says that EPDP team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledgement receipt of a SSAD request should be without undue delay, but not more than two business days from receipt unless, one, [inaudible]

circumstance does not make this, or, two, the SSAD is implemented using technologies which allow instantaneous responses to the disclosure request, in which case the acknowledgement of receipt must be instantaneous.

One thing that staff did observe here – we didn't apply a change here yet – is that we're now talking about a centralized gateway which would be receiving requests, which, under our assumptions, means that it's under Numerical 2, that an instant response would be received. I think that's a separate notion from the comment that was made. There was a comment from the GAC, and it notes urgent request – with a definition – require a different system. Consider ensuring that normal business hours are prominently posed on the relevant website, along with a dedicated contact number of the exclusive use of urgent requesters to contact the potential disclosing party and notify them of the request. We should also consider how urgent requests should be handled after normal business hours.

Staff – our leadership – noted here that the registrar accreditation agreement already maintains requirements for reports of abuse of use in Section 3.18. I'm not going to read that out. We also noted that the SLA for urgent requests is dealt with in the response requirements, and an updated SLA for urgent request is included in the Chameleon proposal section.

So one consideration for the group here is that you may want to consider adding language to that section that specifies that contracted parties should post our business hours on the relevant website, along with contact information for the exclusive use of urgent requests to address the comment that was made. We

noted that that might be something that the group wanted to discuss or consider. I think it was the contracted parties that wanted to talk about this one.

JANIS KARLKLINS: Let us start. James?

JAMES BLADEL: Hi. Thanks. I think that we can live with most of this. I think it's actually a good idea to require posting a business hours and relevant time zones. That's probably what we should insert: business hours and time zone.

But here's the thing. We talk about having some real-world experience with policies. Here's some real-world experience we'd like to share. The 2013 RAA required us to publish an e-mail address for receiving complaints of abuse in WHOIS associated with every WHOIS lookup. Immediately that e-mail address became usefulness. It was full of tens of thousands or perhaps hundreds of thousands of messages per day, usually spam themselves, but requests of abuse like, "I don't like your T.V. commercials," or, "I think you guys are all going to burn in whatever punishment my religion calls for," or whatever. Finding actual, legitimate points was becoming like finding a needle in a haystack.

One of the things that we have deployed is that there's a bounce-back. So, when you send an e-mail address to that required system, it would say, "Hi. This is an unmonitored e-mail address, but here's some links where you can fill out submissions of reports

for different types of abuse. For spam, go here. For malware, go here. For intellectual property, go here." We found that that's essentially a spam filter for that e-mail address.

The net result is it's very, very tempting and it seems like common sense to say let's compel registries and registrars to post very prominently on their website what the contact information is for the person who handles abuse. But, on the flip side of, that's the best way to ensure that we don't get those reports because they are just buried in a sea of noise.

So we can have that channel. I don't think there's any opposition to having that channel. I think that we want to find a way to make that work, which usually involves publishing in a place accessible to the people using SSAD but not public.

Did we misunderstand this?

MARIKA KONINGS: No, but I think that there's a pretty easy solution here because I think we're … This may be predated, of course – the conversation about the central gateway – but I think the solution here is that, when the requester makes a request, they flag that as urgent request, and the central gateway has that information, which is not publicly posted. But they relay it. The contracted parties are required to communicate to the central gateway the relevant contact information where urgent requests should be routed. That may be a way to address your concern and at the same time also address that there's a specific points where those requests would go.

JAMES BLADEL: If we were to register that information with the central gateway, and the central gateway were to share it with those needing urgent requests, and those requesters agreed not to publish or disseminate that, it can use it—

MARIKA KONINGS: It goes to the centralized—

JANIS KARLKLINS: No, that's not what Marika was suggesting.

UNIDENTIFIED MALE: [inaudible]

JANIS KARLKLINS: Yeah.

JAMES BLADEL: Okay.

JANIS KARLKLINS: There will be, at the portal where you file the information, a box: is this request urgent or not?

JAMES BLADEL: Yes, but—

JANIS KARLKLINS: If the urgent request is ticked, then the central gateway will indicate that this is an urgent request to the contracted party without giving any information to the requester.

JAMES BLADEL: I'm fine with that, but that's not what the … We'd have to change the wording to reflect that.

MARIKA KONINGS: It can be [reworded].

JAMES BLADEL: Conceptually [we can.]

MARIKA KONINGS: Yes.

JANIS KARLKLINS: I have Laureen, then Mark Sv, and then—ah, okay. Please.

[VOLKER GREIMANN]: Just a small tie-in. We would also propose to mirror the language for the SLAs to that urgent request very closely to the LEA abuse requests that we already have in the RAA because that will allow us to merge processes.

JANIS KARLKLINS: Marika is nodding, which means she understand.

MARIKA KONINGS: [inaudible]

JANIS KARLKLINS: Laureen, please?

LAUREEN KAPIN: I'm not – oh, James has left the room. Oh, there he is. You're hidden behind Volker from where I'm watching. So I appreciate that you don't want a system that gets filled with garbage because then it obscures the real requests. I'm sorry.

Maybe I didn't understand your proposal, Marika, but the feedback I've gotten from the folks on the front lines of these requests is that they really want to be able to talk to someone at the registrar level to know that someone sees their request and that it's going to be acted on. I'm not sure if your proposal actually results in that because it seems like the centralized authority who actually has no interest in this urgency, really, is getting the information. So I don't know how that solves the issue of, if you're outside of business hours, having some ability to make sure that a live person sees that there's this pending request.

MARIKA KONINGS: If I can respond, I think that's partly captured in the SLA because I think—

LAUREEN KAPIN: It's not.

MARIKA KONINGS: … for the urgent requests, there's a one-business day response, not—

LAUREEN KAPIN: We're talking across purposes because you're talking about the timing of one business day, which, over a weekend, could be at least 48 hours. What I am expressing as a concern is that, if it's a truly urgent request on Friday at midnight, the requester in an ideal scenario is going to want to be able to make sure that a live person has seen that.

MATT: [inaudible] to the registrars.

[JAMES BLADEL]: Yeah.

MATT: Right?

LAUREEN KAPIN: I'm not [inaudible].

MATT: You can go directly to the contracted party, to the registrar. The LEA does not have to go through the SSAD. Right? They can directly contact the registrar.

LAUREEN KAPIN: Right. I understand that conceptually for your savvy law enforcement purposes who know James' e-mail address and friendly Volker, who they can reach out to. But, for your less savvy, connected law enforcement folks who want to make this request, I'm concerned about them. I'm also concerned about the registrars who aren't as responsive as the folks in this room.

JANIS KARLKLINS: Okay. We will finish this conversation [inaudible] you want to say something?

JAMES BLADEL: I'm just—

LAUREEN KAPIN: [inaudible] offline. [inaudible].

JAMES BLADEL: Yeah. Let's do that because the challenge that – we ran into this challenge again; Becky, I think you, Volker, and Matt were starting to have PTSD from the 2013 RAA – we can compel people to publish their contact information and share it with the appropriate folks, but, beyond that, it's very hard to write into a contract that

they answer their phone, that they answer their e-mails, that the respond to the e-mails that they receive. Do you know what I'm saying? It's very difficult to do what you're doing. I'm not saying what you want is not desirable. It is. I think good actors … It's almost saying you will not just abide by the letter of your contract. You will abide by the spirit of it as well, which is to be accessible and to respond to contact requests. We struggled with this.

JANIS KARLKLINS: Okay. First Mark Sv, and then Franck.

MARK SVANCAREK: Thanks. Two things. First I want to agree with Volker that, where we have any timing or [inaudible] – or stuff like that – issues, [it'll all] be put into the SLA thing. It's just crazy how it's all distributed like this. So [we'll put] everything in the SLA thing.

The second thing is that James is giving us an example of an automated acknowledgement receipt. "I have received your request for abuse, blah, blah, blah." I presume that it sends a response in seconds or minutes. So, whenever we talk about these acknowledgements of receipt in the SLA, they've got to be seconds or minutes. Whenever I see one day or something like that, I'm just confused. Thanks.

JANIS KARLKLINS: I think that this is what we're talking about, since this is a portal in the central gateway. So then the acknowledgement of receipt would be sent instantaneously, unless there is some crash or, let's

say, [force major] that does not allow the system to send a response. I think that's the spirit that should be reflected in the recommendation.

Franck?

FRANCK JOURNOUD: Sorry. I'm not quite sure. If we are talking about acknowledgement or receipt, it's milliseconds, period. I don't understand. Whether the request is urgent, whether it comes on a Saturday or on a Thursday at night or during the day, we're just talking about a system saying, "Your request isn't lost in cyberspace. I've got it." No human has to read it. No human has to click "Yes, we received it," or, "No, we didn't receive it." It's all automated. Whether we're using a [beautiful] gateway, RDAP, blah, blah, or whether you're using … We didn't do any of that. It's just e-mail that … God forbid we would stay there. It's all electronic [inaudible].

JANIS KARLKLINS: No. The concern is that, if the urgent request is filed and the acknowledgement is received, then the next step is that, for urgent cases, it is expected that somebody will look at them immediately.

FRANCK JOURNOUD: Right. So it's not an announcement of receipt. Then it's a response. It's an authorization. But it's not an acknowledgement of receipt. So we're talking about a different section.

UNIDENTIFIED MALE: [inaudible]

FRANCK JOURNOUD: I think we're talking past each other.

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARLKLINS: So can we settle that the acknowledgement of receipt will be sent in an automated way after the reception of the request? Something like that.

MARIKA KONINGS: [I think we have to capture that].

JANIS KARLKLINS: Yeah.

UNIDENTIFIED SPEAKER: [inaudible]

JANIS KARLKLINS: But not more than two business days from receipt.

MARIKA KONINGS: [inaudible]

JANIS KARLKLINS: Sorry?

MARIKA KONINGS: That goes out?

JANIS KARLKLINS: Yeah, that goes out. This is what I was saying.

ALAN WOODS: No problem with that. A) It's already in there. But heaven forbid that the SSAD have a technical failure. Are you going to put an [SLA technical failure in and therefore don't get it] out within 15 seconds? It took them a few hours. It's not the end of the world. It's in there already that it should be automated. But let's just give them a little bit of leeway.

JANIS KARLKLINS: I think we're getting too excited about this one. Right? I have five hands up on this. I would say can we move on?

No? We can't? So then I need to follow the line. Volker and then Chris.

VOLKER GREIMANN: Just saying that, even if you have an urgent request, that doesn't get you to talk to anyone. It just gets your request handled earlier. Like I said, we would be happy to use the same standard that we

use for LEA requests under the RAA that's currently in place for those, which would be the 24/7 approach for those urgent requests as defined in our current draft.

JANIS KARLKLINS: Chris, please?

CHRIS LEWIS-EVANS: Thanks. To be honest, I think we're getting hung up here because this was written when we were talking about three models. We've now got one model, he says, hopefully. I just think this needs rewriting to reflect that.

JANIS KARLKLINS: This was what I was trying to suggest. Maybe it didn't come through very clearly. So we will do that.

Next is 45.

MARIKA KONINGS: Issue 45 is in response to the response requirements recommendation. The current language there is, "Responses for disclosure of data in whole or in part which has been denied should include rationale sufficient for the requester to understand the reasons for the decision, including, for example, an analysis and an explanation of how the balancing test was applied, if applicable. Additionally, in its response, the entity receiving the access disclosure request must include information on how public registration data can be obtained."

I'm just noting here that we should change that to the central gateway. There was a suggestion here from the IPC: We should insert language akin to that in the privacy proxy policy. Disclosure cannot be refused solely for lack of any of the following – a court order, a subpoena, pending civil action or a UDPR or URS proceeding – nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name."

The NCSG provided a response here. "I see no reason for our policy to categorically eliminate what in some cases could be a perfectly valid reason not to disclose – the last part – IP infringement in content on a website."

I think there was also a suggestion to delete the "for example." I'm not really sure if we actually already applied that potentially. I think there was also a suggestion to insert, "If the request was denied in whole or in part because the requested data is already publicly available, the response should indicate exactly where." I think that was already something captured as well.

So there's some concern over whether providing those reasons could maybe go too far because that would basically exclude those reasons for refusing a request, which, in each case, may be different. There may be cases where that may be valid reasons. So that's why at least from the staff side we didn't feel comfortable adding that language, also noting that there was some concern expressed by others. So this is obviously one for the group to consider whether that's something everyone feels comfortable adding or not.

JANIS KARLKLINS: Margie, please? Your hand is up.

MARGIE MILAM: Brian was first.

JANIS KARLKLINS: Sorry?

MARGIE MILAM: Brian is first.

JANIS KARLKLINS: Brian is first? Brian?

BRIAN KING: Thanks, Janis. This language we didn't just make up. This is from the privacy proxy consensus policy. The concept here is that, if we've agreed as a community not to allow these as blanket reasons for rejection based on nothing more than these reasons, we've agreed that these aren't good enough and play lip service to the requester. So these responses are not allowed in a reveal request of privacy proxy of the underlying registrant data. So, if that's good enough there, that should also apply to redacted WHOIS data. So it's the same concept there. It's important that these types of responses just indicate that that the request has not

been reviewed or considered are not going to be acceptable reasons to deny a disclosure response. Thanks.

JANIS KARLKLINS: Okay. Margie, please?

MARGIE MILAM: We agree with what Brian mentioned. Just so the folks that don't submit request know, this is a common occurrence. You'll get blanket responses from some registrars that will never provide data based upon "Go file a UDRP" or "Go get a subpoena." So it effectively defeats the entire purpose of the system if that can be the default answer at all times for every request.

What we're talking about in this system that we're hopefully building is one where that kind of scenario is no longer possible and that there are scenarios where there would be disclosure. So this language – all it really does is say that can't be the only reason you don't disclose it. If there are other reasons that apply, then you can still say no. But it shouldn't just be the default answer in all cases. That's what we're trying to address.

JANIS KARLKLINS: Thank you. Now I have Volker, then Franck, and then James.

VOLKER GREIMANN: Thank you. Well, we are happy with the current language. We don't believe that this edition is necessary. We should also consider that the Privacy Proxy Accreditation Working Group's

results were all pre-GDPR. So GDPR didn't fact into the consideration at that time, so any requirements were set out at that time will have to be looked again under the lens of the GDPR. That's one thing.

The second thing is that it may be simply the case that, in certain jurisdictions, you have to this kind of justification for disclosing private data to a third party requester. Therefore, asking for a court order or a similar subpoena or what have you may be the correct answer that you would be getting in any case as well.

So I don't see the need for the edition at this point.

JANIS KARLKLINS: Okay. But maybe think if there is any way to accommodate the concern or response to the concern of the IPC and the BC, not immediately. But I think we need to look also in that spirit.

Next is Franck, followed by James and then Alan.

FRANCK JOURNOUD: I'm sure I have just a solution that will take care of all of the concerns that NCSG and my friends from the contracted parties would have. The operative word in Brian's language is "solely." So you can't just say, "You mentioned intellectual property. Sorry. It's a no." You just decide solely for that reason. You can't deny just by saying, "I'm sorry. I always ask for a subpoena. I never give out data without a subpoena." You can say, "Well, we've done a balancing test and given the rights, blah, blah, blah, but, if you have a subpoena, it's different," or, "Well, this type of IP-related

request we denied, but this other type?" So you need to go beyond just, "Sorry. IP. Go fish." "Solely" is, I think, the operative and critical word in Brian's language. And there you go. Problem solved.

JANIS KARLKLINS: [inaudible]. James?

JAMES BLADEL: Thank you, Janis. Thanks, Franck. Actually, that is helpful – a little bit. Just a quick thought here because I think that, in some ways, if I read a response that says, "Before I can provide you this information, you must provide a subpoena," or court order to warrant, etc., to me that is a rejection. The respondent is essentially giving you other options to essentially appeal the rejection or overrule the rejection. But it's a rejection. So I'm concerned. Maybe the word "solely" will fix this, but I'm concerned that this is saying you can't reject. Or are you saying you can't reject unless you tell me the justification for the rejection? I'm just struggling with this.

I do agree with Volker. I think that bending the EPDP to conform to something that was in the privacy proxy spec to me seems backwards. The privacy proxy spec is pretty old by now and needs to probably be updated to reflect whatever we come out with here because there's a lot of different policies that were stuck pending the adoption of GDPR, and now California. It feels like, if we're going to fix something, we should fix them all with some sort of a consistent approach.

So maybe we can fix it with the word “solely” or flip it around and say, if you’re going to reject a requests, you must provide a justification for that rejection and offer whatever alternative channels that might be available, like a subpoena, a warrant, UDRP, or whatever, and then list them as other methods maybe because, as it reads now, it’s almost like we can’t reject requests.

JANIS KARLKLINS: Thank you, James. Alan, followed by Mark Sv.

ALAN WOODS: Thank you. Two points. The first one is that I’ve seen a good number of requests coming through, specifically where, in fairness, they’ve been easy enough. But the actual request itself does not normally give any detail beyond which I would need for a 61F, just purely because it doesn’t tell me why you need that data. It just says, “I have a trademark. Give me the data.” That’s across the board what I get. “I have a trademark. Give me the data,” not why you need the data.

That brings me onto my second point. Because we’re here at the face-to-face and we have a lot to get through, let’s just call a spade a spade and bluntly ask the question: why do you need the data? Why don’t you get it in the discovery? That’s the question. Why don’t you use those things? Because things brings up in my mind questions of necessity. These are things I have to, in a very GDPR-specific world, contemplate. What is necessity? And what is the necessity for you in that instance to [get data] from us as

opposed to through other obvious legal processes? That's something that's important.

I'll just leave with you with – I'm going to be that person; I'm sorry – what the Irish data protection commissioner brought out in December of last year with regards to that. They said, in light of this, controllers should make sure that any processing of personal data which they undertake or propose to undertake is more than simply convenient for them or potentially useful or even just the standard practice which they or the industry had used up until now. That's what we're talking about. You need to justify it in the instance. You can't just rest on your laurels. That's it.

I see Franck is jumping off the chair. But that's it. I ask the question, why do you need it?

JANIS KARLKLINS: If I will not give now the mic to Franck, then we will suffer. Franck, please go ahead.

FRANCK JOURNOUD: My mother would agree. It's [totally good you] … But it seems that you're commenting on current experience. We're talking about a policy. We're developing policy. We, I think, pretty much agreed on the request requirements. We need to justify a request. We can't just say, "Hey, I got a trademark, so give it to me." It's like, "I have a trademark. The domain is infringing on this trademark? How?" I should that I in fact legally own this trademark and that I'm not making it up, etc. So, if we have all these justifications, it seems to address what you were saying. So, if we have all these

justifications, then you can't just say, "Eh. Give me a court order. Give a subpoena." I think the policy should say, no, we don't need a court order when we've justified all these requests.

UNIDENTIFIED MALE: [inaudible]

FRANCK JOURNOUD: What's that?

UNIDENTIFIED MALE: [inaudible]

JANIS KARLKLINS: Go ahead.

ALAN WOODS: But we can't change the law. That's the legal requirement of necessity. I'm reading what the Irish DPA is saying: you have to consider these things when it comes to necessity. Are there any other less intrusive ways in which they can get that data? To me, a legally established process of you establishing your trademark in a court is one of those less intrusive means because it's something that is objectively known to a registrant: if I infringe on somebody's trademark, then they can get that data to a court process, not necessarily from the … Again, I'm not saying this. I'm just saying this is the interpretation of what is being said even from my local DPA.

So, again, the question is, what makes it the least intrusive means of getting it when there are other means of getting that data?

JANIS KARLKLINS: I have Mark Sv, Brian, and Margie in line.

MARK SVANCAREK: So many things. Let me get my thoughts back together again. Sorry, Alan. You threw me for a loop there and now I've lost my train of thought.

JANIS KARLKLINS: You can wait. I will give it back to you.

MARK SVANCAREK: Yeah. Give it back to me. Sorry.

JANIS KARLKLINS: Brian, please?

BRIAN KING: Thanks, Janis. And thank you, Alan. I think I agree with a lot of what you just said in that the concept that we're trying to address here is that the registrant data is unavailable in many cases. When we go through the effort and trouble to put together the best damn request you've ever seen – the most detailed, all the reasons, and it's the best use case (in our mind, that happens often; in your mind, it might happen less often than we think it

does) – we submit those requests and we're often met with, "Come back with a warrant." That's an unacceptable outcome for this.

In the scenario that you outlined, if somebody made a less-than-full request in those scenarios, I would expect that you would reject it. But your response would not be, "Come back with a warrant." Your response should be, "You haven't given us enough information," or, "There appears to be a less intrusive means." It's not stiff arming. "Come back with a warrant. We don't give data unless you have a warrant or a subpoena." But those are the responses that we receive today all the time. They say, "If you want this, you have to file a UDRP." "If you want this, if you have to file a warrant."

What we're looking for here is to just eliminate those and to keep the other side – the parties that we're counting on to do that full review that you do and Volker and everybody does … But you're in the minority. Many registrars ignore or respond with, "We don't give out this data." That's just an unacceptable outcome. It's not one that we can live with. Deny us all day long for good reasons: if the request is faulty, if there's a less intrusive means. Whatever good reason. But these are the types of things that we do receive all the time, and they're just unacceptable to receive when we've taken the time to make a valid request. So that's where we're coming from here. Thanks.

JANIS KARLKLINS: Thank you. Margie?

MARGIE MILAM: I think we have issues. If you think about what Alan is really saying, he's saying you have to file a lawsuit before you get the data. But you don't know who to sue and where to sue and whether you have a legal claim. That's the problem with the position that you're articulating. GDRP does not require a subpoena in order to find that out. I believe there's a section – I'll have to look it up – to be able to investigate legal claims. That's what we're really talking about. If we go through all this work and we get the answer at the end of the day of, even though we have our trademark, we've given our reason we need, we filled the form correctly, and there's no other place to get the data, "You need a subpoena," then this system is not going to work. It's just flat-out not going to work for our constituency. There has to be an acknowledgement that there are scenarios where a subpoena would not be required for civil claims. I think it's in GDPR. I just have to find the section. I don't know if anybody knows it off the top of their head, but it's there.

JANIS KARLKLINS: Okay. Mark, are you ready now?

MARK SVANCAREK: Yes. Sorry about that. The first thing I was going to say, back when I jumped in the queue, is that I have one concern about the proposed language. It's that I don't believe that it belongs in this section. This sections is about response requirements, and you have to say why you're denying it. I think the proposed language

is good and should be somewhere in our policy. I just don't think it belongs in this particular paragraph. So that's a slight deviation from the rest of my constituency.

To what Alan is saying, yeah, we will be creating a policy where we have to give our explanations. I don't know why it was so hard for us to explain it, but Margie has explained it there. There is a difficulty in the whole process if we can't get at least some of the data up front. It is pretty hard.

I do think that the statistics that are generated by the portal are going to show whether or not this is an issue. We just want to make sure that, if we do find that there are some parties for which this an issue – a consistent, persistent, intransigence to deal with certain classes of requests – we'd like to have some recourse to it. That's why I think having this language somewhere in our policy will be important.

But, yes, we should also consider that the request should be complete and justify why we need the data. So that should be assumed. If it's not clear, we should reiterate that. Thanks.

JANIS KARLKLINS: Chris?

CHRIS LEWIS-EVANS: Thanks. Hopefully I can pull this back somewhere we can get agreement on this. I think James summed it up quite well. Saying you need a court order or subpoena is another method of getting that data. It's not the SSAD. You don't file an SSAD request and

attach a subpoena to it. If you're going to serve a subpoena, it's not going through the SSAD. So saying you need a subpoena is not a reason to deny a request. It's an alternative method of getting the data. Yeah?

It is. It's an alternative method of getting the data that we're asking for. What the wording here is trying to get at – this is, I think, what Franck said – is they don't mind saying you need a subpoena, but why do you need a subpoena? As Volker said, is there some local law that, for the release of the data for the purpose, says you need a subpoena? If that's the reason, I am sure colleagues over there will fully accept it. If it's because you don't quite might the balancing test because they're a protected individual and to get the data you'd need a subpoena, that's fine. All I think we're wanting is that it's not – this goes back to that "solely" word – solely the reason. It's a flat-out "You need to get a subpoena to get access to data." "Why are you saying that we need to get a subpoena to get access to the data?" "It's because of local law/It's because you haven't given us enough information/It's because they're a protected group." You might not want to say that. You might say, "You don't reach the [bar]."

Do you see what I'm trying to get at? I think that's what we're covering off: we need a proper reason for the non-disclosure of that data so we can understand, yes, the right next step that's least intrusive is to and get a court order because – face it – a court order or subpoena is normally more intrusive than a simple SSAD request, where you can say you only need this, this, and this piece of data to fulfill because, when you get a court order, you tend to get more data. I'm just saying generally.

So I think it's just a way of explaining where we don't meet the bar for the request. I think everyone accepts that there will be cases where the correct answer is you need a subpoena, but I think all we want is "because." Does that make sense?

JANIS KARLKLINS: After listening to all the arguments now, my questions goes to the CPH. Is there any way how you can accommodate concerns?

Please.

JAMES BLADEL: I think we're really close to violently agreeing with each other, in listening to Chris. Or maybe not violently agreeing with each other. I'm sitting next to a two-meter German. You're right. What these are enumerating methods of getting the data. The existence of alternatives does not constitute a justification for a denial.

So what we should say is, "This request has been denied. Reason. Here are some alternatives you can try." If that was the formulation of a response, then I think everyone gets what they want because I think the word is "solely" or "exclusively." You can't cite the fact that alternates exist. Now, I'm looking to the European privacy lawyer three doors down to tell me that I'm not coloring outside the lines here, but it sounds like you could say, why? "Your request failed the balancing test. Go get a subpoena, warrant, court order, or file a UDRP." Something like that. But it can't be because you could get this information through these other methods [we reject] because I think we're fixing it. But it's a pretty big rewrite.

JANIS KARLKLINS: For the moment, I do not see how are fixing because you are arguing exactly what is written in the middle column. That is not what Brian is suggesting.

Alan and then Volker.

ALAN WOODS: Sorry. I'm probably jumping in the queue again. My problem here is just with the exclusion of that as a reason in this wording that is proposed here: that the exclusion of having saying you can get a subpoena. That is actually is a balancing test. If you failed a balancing test, one of the reasons for failing the balancing test is that this is a least invasive way of doing it. It's not invasive to me. It's not invasive to them. It's invasive to the registrant and it's to the data subject. My problem is that I don't like the concept that we're being told that we can't deny for a reason that is very valid under the law. If we get to a place where we can agree – that is where you can't just deny, blandly saying, "Get a subpoena"; you need to give an example as to why you believe that that is considered to be a less invasive method … Is that what you're saying? Give us more background as to why we believe that is a less invasive method? Or are you saying you can't just use that as a reason for denial point blank? Because I can't accept that.

But I can accept if it's like, "This is a reason. You can get a subpoena. You can get disclosure. You can get discovery for these reasons based on our reasoning." Then you can always

dispute that. You can always appeal what we're saying. Also, you can always go to the DPA and say, "Is this valid?"

All we really need … Actually, let's be honest. This is going to turn moot very quickly once that is brought to a DPA at some point in the future, and they go, "Yes, that is a valid reason," or, "No, that isn't." And then everything changes. But we're working in hypotheticals here. I just don't want us to not be allowed to use what is a perfectly valid reason for a denial of disclosure.

VOLKER GREIMANN: I think the best solution, from everything I heard here, is to just add some paragraph to the front of this clause that basically states something to the effect of, "Absent any legal requirements to the contrary, disclosure shall not be denied," because, ultimately, if there's a legal requirement that you have to have a court order, than that can be the sole reason for refusing the denial. So, if we have that as a legal requirement – that you have to do that instead of us providing that data – then that would be the valid reason. If that is not the case, then we'll just follow the lines that Brian suggested.

So I think, if we add that caveat in front of that language that you have proposed, we could agree with that. That would encompass your considerations and James'. I think all the edge cases would be covered as well.

JANIS KARLKLINS: I'm now looking to the sequence in the recommendation itself. What this speaks to is the response requirements for contracted

parties. I'm referring to Page 14 of the model. The first paragraph suggests that the disclosure response must be provided without undue delay, and then in line with the SLAs outlined below.

The next paragraph suggests that the response where disclosure data has been denied should include the rationale for denial and then, additionally, in response, the entity receiving the disclosure request must include information on how [helpful accreditation] can be obtained.

So there is a logic in that. So what is requested probably does not belong to this particular section but rather [as a] safeguard in the section on how the decision is made: that decision should be denied solely because it is A, B, C, D. Right?

So think here we are fine with what is written, but we need to make a note and see how that concern could be accommodated in the sequence. On the fly, I cannot do it, but I would suggest that we note this point. Maybe we can come back to it even today but leave this as is because it speaks as: if the request is denied, then you need to say why it is denied and where you can get public information.

Would that be okay?

Thomas, you are impatiently waiting.

THOMAS RICKERT: I might be. It's been a long day already. I think that we're discussing two things that are legally not related to each other on the subpoena thing. If you have a subpoena, law enforcement or

any other public authority has a right to request data from the contracted party, in this case. So the contracted party is obliged to proceed that data based on 61C, right?

UNIDENTIFIED MALE: [inaudible]?

THOMAS RICKERT: Yes. They have a legal obligation to disclose. We're now back to one issue that I raised earlier, that this conflict between 61C and 61F, where it is easier to disclose to a law enforcement authority abroad that doesn't have a legal basis for the domestic contracted party … But, as we know from Ruth's advice, she thinks – Chris, you've been saying this as well – you can then use the 61F balancing test to see whether you want to disclose.

So I think where 61C is concerned you have to provide the data, not questions asked, unless you want to challenge it in court. But I think that referring somebody to a subpoena is not a justification that has anything to do with the balancing test. I don't think it's less invasive. It's just a different angle because one forces you to give the data and the other one gives you the option to do the balancing test before you take the risk to disclose the data.

So maybe we can proceed by just dealing with these separately. I'd not say you could have chosen the subpoena, which is a less invasive mechanism, but just do the balancing test if you consider to disclose. If the balancing test is in favor of not disclosing, you just don't disclose. Then, as a means of service, you can tell the public authority, "You might check to see if you have the legal

basis based on what you can issue a subpoena for," but that is, I think, unrelated to this.

UNIDENTIFIED FEMALE: [inaudible]

THOMAS RICKERT: But you can't use the subpoena, I think, anyway.

[MARGIE MILAM]: No. We can subpoena if we have a lawsuit. If you're in an active lawsuit, you can subpoena. But the point is that that shouldn't be the requirement for getting WHOIS access because you don't know who to sue until you've gotten the WHOIS information. So it's backwards to say you have to have a lawsuit and you have to use your subpoena power under the lawsuit to get access to WHOIS. If that's what the contracted parties are saying, that's a huge problem for us. This SSAD will never solve the problem. I hope that's not what we're saying.

The reason why I raise it is because that's actually what we're seeing from many contracted parties. I know that people here at the table are doing different things. I appreciate the effort that a lot of you put into these requests, but the reality is that there are contracted parties that routinely do not look at requests. All they say is, "Go get a subpoena," or, "File a UDRP." That's not the answer that's going to work for us.

JANIS KARLKLINS: I can only reiterate my proposal. Here we're talking, in this paragraph, #45, about what information should be provided in the response of denial. I think that this is exactly what we expect to receive: the reason why this request is denied.

I'm looking at the disclosing-decision recommendation, and that is Recommendation #6 on the authorization provider. I think that here there is a passage talking about denials. If you would agree, since we probably will review this section tomorrow … I'm now just looking. So we could already include the proposal that IPC folks are proposing in this section that – yes, Brian?

BRIAN KING: Thanks, Janis. If I could add to that, I'd like to include Volker's amendment. I appreciate that engagement and I think that works for us. Especially if that helps our friends come on board, I think we're okay with that. So we're happy to take it up in that section [inaudible]. [I don't know if] that gets us closer. Thanks.

JANIS KARLKLINS: Then we would not go to anything else. That would be sufficient to address your concern, right?

Okay. Marika, do you have Volker's proposal?

MARIKA KONINGS: Yeah.

JANIS KARLKLINS: Could you read it – how it will look? Just making sure everyone understands what our landings are.

MARIKA KONINGS: My understanding is that this language would then go in the contracted party authorization. I think we just need to look for what the best spot for it. It would read something of this nature: "Absent any legal requirements to the contrary, disclosure cannot be refused solely dah, dah, dah, dah, dah."

JANIS KARLKLINS: So we have a solution.

[JAMES BLADEL]: Sorry. I don't meant to ruin the mood, but didn't we also agree that we would relay the reason for disclos[ure] [inaudible]?

UNIDENTIFIED SPEAKERS: That's already in there.

JANIS KARLKLINS: Let us move to 46.

MARIKA KONINGS: 46. There were a couple suggestion for changes here. Staff looked at this. There was originally an "and." There were suggestion that this should change to "or." But, from our reading, that would change the meaning or at least our original intent of

this language. As such, staff suggested alternative wording, which we hoped would address that concerns that were expressed while being explicit on what this means.

So the proposed updated or reworded language would read: “The EPDP team recommends that, if a contacted party determines that disclosure would be in violation of applicable laws and consequently results in inconsistency with these policy recommendations, the contracted party must document the rationale and communicate this information to the requester and ICANN Compliance, if requested.”

There was a suggestion that maybe the “and” should just change to “our.” Our concern there was that, if disclosure would be in violation with applicable law but not result in consistency with the policy recommendations, there wouldn’t be an issue because the contracted party would just reject the disclosure request because it wouldn’t be applicable with local law. So that’s why the “or” from read didn’t make too much sense. It’s more, if there’s a conflict with a local law which results in inconsistency or conflict with the policy requirements, that is the condition under which a contracted party would document that and communicate that information.

So that’s the background to our proposed change and our concern that the “or” would not go to what was originally intended with this action.

JANIS KARLKLINS: Thank you. I have many hands up. My question is, are these all new hands?

I have James, Thomas, and Volker.

JAMES BLADEL: That is an old hand.

JANIS KARLKLINS: Yeah, I thought that these were old hands.

JAMES BLADEL: [inaudible].

MARIKA KONINGS: Volker's is new.

JANIS KARLKLINS: Volker, your hand is new. Okay.

VOLKER GREIMANN: Actually, we like the comment here because there may be situations where disclosure would not be in violation of applicable law but it would still be inconsistent with some of the policy recommendations that we made because of certain considerations of privacy that may not be prohibited but still have found any reflection in the policy. I don't have any specific examples for that yet, but there may be situations where there's no violation of law but there is a violation or inconsistency with policy, and therefore an "or" might be warranted. So we like that proposal there. This is why we flagged this.

JANIS KARLKLINS: Okay. So, if everyone likes “or” instead of “and,” except staff, then maybe …

MARIKA KONINGS: Just playing devil’s advocate here. Wouldn’t that open the gateway to say, “Well, we think there is a reason. It’s not really against the law, but we don’t really like what the policy says.” But there’s some vague reason and we’ll just document it, but it’s actually not inconsistent with the law. But we are not complying with the policy requirements. Couldn’t it open up for that if you say “or”?

VOLKER GREIMANN: The way that we understand this is that, if you put an “or” there, it either has to violate the law – Option 1 – or it has to be inconsistent with existing policy. So the only iffy thing at that point would be the interpretation of that policy. It’s not “we don’t like how the policy is written” because the policy is still governing our actions here.

MARIKA KONINGS: But, if you’re inconsistent, aren’t you in breach?

VOLKER GREIMANN: Therefore, we wouldn’t disclose, yes.

MARIKA KONINGS: Right, but under what reasons? Maybe I'm missing the point. I'm looking a bit to [Dan] more from a legal perspective.

VOLKER GREIMANN: The language says that disclosure would result in inconsistency with policy. So that's what we read here. So, if we were to do a disclosure, that would cause inconsistency with the policy. Therefore, we would be in our rights to refuse to disclose in this case, whereas, if you have an "and" here, it would have to be a violation of law and cause an inconsistency with the policy. That might be over the top. That might be too hard a requirement.

JANIS KARLKLINS: I'm just trying to do the reading. If you have "or," then you can read two sentences and they should be logical. Now I'm trying to do that. "The EPDP recommends that if the contracted party determines that disclosure would be inconsistent with applicable law, it must be documented." The second is, "The contracted party determines that the disclosure would result in an inconsistency with these policy recommendations." So I'm missing the logic there. The disclosure would result in inconsistency of these policy recommendations.

VOLKER GREIMANN: With [inaudible].

JANIS KARLKLINS: If we use “or” instead of “and,” then the sentence would read, “If the contracted party determines that disclosure would be in violation of applicable law or an inconsistency with policy recommendations, the contracted party must document the rationale and communicate this information to the requester.”

VOLKER GREIMANN: Yeah, that’s the second point. We like the original language – the entity disclosing the data – instead of the contracted party. Ultimately, it will be a contracted party, but I think we should focus on what they’re doing here and not what they are.

JANIS KARLKLINS: Okay. In calling names, we need to be consistent throughout the document.

VOLKER GREIMANN: Yes.

JANIS KARLKLINS: Now, in light of our agreement on the model, we need maybe to reflect a little bit internally to see how it would read the best throughout the text.

So what’s the landings on them?

MARIKA KONINGS: [inaudible]

JANIS KARLKLINS: Stephanie and then Brian.

STEPHANIE PERRIN: I think this may disrupt the train of thought that Volker was on, but certainly, if you have an instance in any country where there was no applicable law and the recommendation that we have of having a consistent policy whether you have applicable or law gets mushy as we release, then you are only relying on overall policy in the document to provide rights to people where there is no applicable law. In those cases, you would be well-justified if you did not want to deny registrants in a particular jurisdiction the same human rights protection that you would have anywhere else. Then you're going to deny the request on those grounds. That requires an "or" because, otherwise … We had quite a bit of discussion at this end of the table about how confused we were with the wording generally. My concern is, as always, that, if we put this out for comment, we're going to get a dog's breakfast anyway. We have to be clear. So, if we don't understand it, nobody else will.

So I think it requires a bit more detail and clarity here just to take that, but I think that's a valid example of why you need "or" and not "and": obviously, compliance with the law is part of our policy. Right? I hope so. Otherwise, I'm going home. So you don't need the last half of that sentence unless it's different. Right? Therefore, it's an "or."

JANIS KARLKLINS: Can we land then on “or”? I think Brian is in agreement. Yes? But then this “or” should be …

UNIDENTIFIED FEMALE: [inaudible]

JANIS KARLKLINS: No, no. Again, you need to read the sentence in the context. So we have in this section on the response requirements three requirements for the contracted parties. Then this comes as an addition, which suggests that, if the entity disclosing the data determines that disclosure would be in violation of applicable law or result in an inconsistency with policy recommendations, the entity disclosing the data must document the rationale and communicate this information …” Rationale of what? Rationale of …

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARLKLINS: I think here there is one word missing. “must document rationale” of what?

UNIDENTIFIED MALE: Denial.

JANIS KARLKLINS: Of denial.

UNIDENTIFIED MALE: Yeah.

JANIS KARLKLINS: "and communicate this information to the requester and ICANN Compliance." So let's land on this one. I think then that sentence reads … okay.

VOLKER GREIMANN: Just a …

JANIS KARLKLINS: Yes, Volker?

VOLKER GREIMANN: This is a bit of digging in an already-settled matter, but do we really want ICANN Compliance to receive a ticket for every denial that's issued? That's what this says, that, every time there's a denial, "Hi, ICANN Compliance. Here you go." They would be swamped. It's just a point of realism here.

JANIS KARLKLINS: Yeah, but here is, in the brackets, "if requested." So that is—

VOLKER GREIMANN: [inaudible]

JANIS KARLKLINS: … safeguard. This is not a requirement.

VOLKER GREIMANN: Okay.

JANIS KARLKLINS: Okay. So we settled then 45, and that will be reflected. Now we go …

MARIKA KONINGS: [inaudible]

JANIS KARLKLINS: [Was it?]

MARIKA KONINGS: [inaudible]

JANIS KARLKLINS: Yes. So now we go to 53.

MARIKA KONINGS: 53 currently reads: “Where required by applicable law, [inaudible] must provide mechanism under which the data subject may exercise its right to erasure.”

What the staff language added here is “and any other applicable rights,” because some of the comments pointed out that there may be other rights that are relevant here. I think it was SSAC, if I’m not mistaken, that had a concern about this one.

UNIDENTIFIED MALE: Well, not really a concern. I actually just missed that you had proposed additional language. We just wanted to make sure that the other applicable rights were mentioned as well, just for the sake of consistency.

MARIKA KONINGS: So just to clarify, you would propose to spell them out? Or in this way it’s sufficiently clear that there may be other rights.

UNIDENTIFIED MALE: I’m perfectly happy with it as proposed.

MARIKA KONINGS: Okay.

JANIS KARLKLINS: So who then raised the issue with 53?

MARIKA KONINGS: I think it was [inaudible].

UNIDENTIFIED MALE: I did, but it was based on not realizing that there was additional language. I was looking at the comments from ISPCP and agreeing that that should be in there. So I apologize for missing that.

JANIS KARLKLINS: No worries. So then we're done with 53 and we can go to 56.

MARIKA KONINGS: 56. The current language reads – and this relates to the confidentiality of requests, where I think there is anyway going to be a little bit of additional work that I think we need to consider separately when … No additional work? Okay.

JANIS KARLKLINS: [inaudible]

MARIKA KONINGS: Okay. Well, I'll read through it and you can comment that. But it was flagged as to whether or not this needed further work. There's a proposed change here. There was a suggestion from the IPC to change some language here. "The confidentiality of disclosure requests. Data controllers of RDS data must inform this" – [originally read] – … "make it clear to …" Now it would read, "Data controllers of RDS must inform data subjects of the types of

entities – third parties – which may process their data. Upon a request from a data subject, the exact processing activities of that data within the SSAD should be disclosed as soon as reasonable feasible. However, the nature of legal investigations or procedures may require SSAD and/or the disclosing entity to keep the nature of the existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority and/or" – that's still language that's in brackets, so some recommendation there and how to deal with that would be helpful – "in accordance with the data subject's rights under applicable law."

I don't recall who expressed concern about the proposed change.

JAMES BLADEL: Well …

JANIS KARLKLINS: Please, Jim, go ahead.

JAMES BLADEL: Just that this is something that Chris and I had to take away as homework a long, long time ago and we're just discussing the importance. I think the IPC addition of "inform" is a good one, that folks should understand exactly what types of request the SSAD will respond to and may share their data with. I think that we want to be clear that there's no affirmative obligation on contracted parties to notify data subjects that someone has requested their information. However, if they ask, we should disclose that.

We did have a discussion, however, on whether or not law enforcement requests should be included in that disclosure and whether or not then that's when we would ask our friends with badges to whip out there special powers and prevent us from disclosing that if they wanted to. Otherwise, they should assume that they would be included in that disclosure.

So I think that's where we landed. I don't know. Stephanie or some of the folks in the NCSG had an issue with some of that, but it seems like we're trying to navigate these very tricky shores.

STEPHANIE PERRIN: Yes, I think we did have quite a discussion about this. Let's be clear here. This language says, "Data controllers of RDS data must make it clear to or inform data subjects of the types of entities – third parties – that may process their data." So this is really the openness provisions in the data protection legislation that requires you to make sure that your registrants are aware of who potentially could get their data.

Now, if you say "inform" – I'm literally reaching back to an example of the Reader's Digest lady who said, "If you inform your readers they have a right to request their data in 8-point time at the back of your magazine, trust me, they'll never write you." That's the kind of abuse of these requirements that has taken place. There's been a long fight and debate for the past 20 years over short notices versus 75-page contracts of [inaudible] that Apple and other send out.

So we're really looking for clarity. The threshold, as I pointed out in Montreal, in [inaudible] it's manifest, enlightened, and informed consent. So these openness provisions are attached to your consent. It has to be enlightened consent.

Therefore, I would caution against slipping into the word "inform." I'm sure it was done with the best of intentions. You don't want to be under any presumptive obligation to ensure that your public, your customers, understand things because God knows I don't know and I'm supposed to be smarter than the norm. I don't understand what's in there or where things might go.

However, better efforts need to be made. So we would like to see other language than "inform." I think "must make it clear" isn't bad. I don't think that means that, if we did a survey, and 50% of your registrants didn't know yet that you are in default but you've made an honest effort of who could inform of them who could potentially get their data … Have I made myself clear on why we object to this? It's an important point.

JANIS KARLKLINS: Stephanie is suggesting to keep the original language – "make it clear to" – instead of "inform." The question is to Brian: can you live with that? I think this is a little bit of linguistics rather than … We're talking about 56, Brian. I understand that it was the IPC who was suggesting to replace "make it clear to" with "inform." Stephanie is arguing that "make it clearer to" is clearer.

BRIAN KING: "Make it clear" is less clear because it's subjective." "Inform" is something that can be done. It's in the notice. They're read it. They've agreed to it. They've been informed. "Make it clear"? I don't know. How well do they understand the English language? That's far more subjective than "inform."

JANIS KARLKLINS: Okay. "Clearly inform." Franck?

FRANCK JOURNOUD: The confusion in my mind and the reason why I had suggested "inform" is because the sentence is about not which specific entity has requested your data but the types of entities. So it seemed to me like clearly we're not talking about in a response to a request from a registrar. We're talking about a disclosure.

I totally take your point that disclosures that are like 5,000 pages in small-font legalese, etc., may not really pass muster of enabling informed consent. So I think we're talking about standards of disclosure. The problem then is there's a lot of different applicable law, given the subject matter of that disclosure, how it needs to be provided, what font, what pop-up on your screen versus if it can be in 20-odd pages, can it be together with other send things you can send too or it should be separate, etc. As you know, privacy law gets really difficult there.

JANIS KARLKLINS: Let's stay focused. This is just probably a legal question and there should be lawyers around the table. So what the legally more

sound verb to make sure that each registrant knows that it is not just the registrar and the registry who will process their data but there maybe be also third parties? So what is the verb that would most clearly ensure that registrants must be informed, must know? This shouldn't be an issue.

Alan, you always come up with good suggestions.

ALAN GREENBERG: I'm not going to come up with a good suggestion because the reality is, even if you have a pop-up and you cannot take it off until you scroll to the bottom, which some of them do, you cannot guarantee that they're reading it. The reality is you can't make sure they know. All you can do is present it to them in something that is not 0.3 font or 0.3 … I can't even get the words out.

STEPHANIE PERRIN: 8-point [inaudible]

ALAN GREENBERG: Well, I was talking about 0.1 point—

JANIS KARLKLINS: You don't have a solution. But do you have [one]?

JAMES BLADEL: Yes.

ALAN GREENBERG: But I think you're right. Is there a term that is used in legal contracts that we can refer to here?

JANIS KARLKLINS: Lawyers, please. Hadia first. Thomas after. Oh, and James. James was first. Hadia and Thomas.

JAMES BLADEL: I don't know what's going on. It's just that this is very similar to something that we had when we went to the RAA. We were talking about counting how many clicks to get to the [rights]. So what would say is something like, "prominently display," "clearly disclosure," or include in their terms of service the types of categories …

I understand, Stephanie. You make a valid point. Apple has trained us not to read these things but just click Yes so you can get to the good stuff. But introducing that onto this table I think just takes us off the edge. I'm sorry. It's a problem no one has been able to fix. But I think that we can address it with some of those verbs like "clearly disclose," in their terms of service or in their registration agreement, which is a defined document: their domain name registration agreement.

We'll put it on the list. We sell 100-and-some country codes, and everyone one of them says, "Put this in your registration agreement. Put that in you registration agreement," so, when you get to the end, there's all these provisions of all these things people don't read that we have to have in there. So let's just put it in there and hope for the best.

JANIS KARLKLINS: So: The confidentiality of the disclosure requirement. The data controller of the RDS data must … Thomas?

THOMAS RICKERT: If you want legal clarification, data subjects must be informed about the data processing in accordance with Article 12 subsequent [PP] because that's the section in the GDPR that spells out all the requirements on how data subjects must be informed.

JANIS KARLKLINS: We're talking here maybe in more general terms, not specifically referring—

THOMAS RICKERT: You can't be more general than that.

JANIS KARLKLINS: Okay. Let's see, Brian, what you have to say.

BRIAN KING: I'm sitting back and smiling because I think we said "informed." I think that's what we suggested there. Doesn't that do it?

THOMAS RICKERT: Sorry, but Article 12 and the following articles say exactly what you need to inform the data subjects about. So that contains the full enchilada. Can't add more.

JANIS KARLKLINS: Basically, referring to another document pushes the customer even further away from information because no one …

THOMAS RICKERT: No. Sorry. I beg to differ. We've criticized that on our comment on the initial report: sometimes we pick and choose individual items. But, if you only inform about those, that doesn't make things compliant. For example, we informed about the right to erasure and the right to rectification, but we leave out the other rights that the users are entitled to, while, if you say Article 12 PP, that tells everything because then you can go to the GDPR, which we reference to as an additional source of information, and that's unambiguous.

JANIS KARLKLINS: What if we say that the data controllers or RDS data must clearly indicate to the data subject the types of entities/third parties which may process their data? "Must clearly indicate to the data subjects."

MATTHEW CROSSMAN: I like Thomas' suggestion. I think thought we might want to take it up a level because we know, for example, that under the new

CCPA, the California privacy law, there are actually additional disclosures that you have to make if you're, for example, selling personal data. So I like that suggestion of "consistent with applicable law" rather than just limiting it to GDPR in order to future proof.

JANIS KARLKLINS: I think Thomas referred to Section 12 of GDPR.

MATTHEW CROSSMAN: Right. I'm saying "applicable law." So take it up one more level so it's inclusive of some of us who may have obligations under the California privacy act, for example, which has different disclosure requirements. It has many of the same disclosure requirements but has some that are very different that are in addition to GDPR.

THOMAS RICKERT: Sorry. When Alan tasked me to go through the entire report to make clear that we're doing GDPR, I think we can achieve what you're trying to achieve by saying "applicable law." But the information [to do it] is according to 12, and subsequent articles of the GDPR are the minimum requirements. So, if you have additional information requirements under applicable laws, then you can add to that. But every contracted party must as a minimum fulfill 12 PP.

JANIS KARLKLINS: We started – okay, Alan. Please go ahead.

ALAN GREENBERG: Sorry. We've changed the subject along the way.

JANIS KARLKLINS: No. This is exactly what I was trying to say—

ALAN GREENBERG: No. Thomas is talking about what we have to inform them on, not the verb we use to inform them, which is what we were talking about until then. I'm happy to stay here forever and talk about this, but—

JANIS KARLKLINS: No, no, no.

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARLKLINS: No. Let's concentrate. We still have half and hour to go and we need to finish this part of the section in order to get something meaningful for tomorrow morning on the text.

Georgios, you haven't been given a shot yet.

GEORGIOS TSELENTIS: Just because I read the article that Thomas was saying, and I saw a part that may help us add some qualifications in what we are

seeking when we inform. It says in the article, “in a complete, transparent, intelligible, and easily accessible form, using clear and plain language.” So there are some bits there that maybe we can quote from article of GDPR and then help with what we mean about clarity here or information. So, if we can add it to the text, I think just copy-pasting from the article might help, if you agree.

JANIS KARLKLINS: Yeah. Could you put that in the chat, please?

GEORGIOS TSELENTIS: I did.

JANIS KARLKLINS: You did already. What we’re trying to say in this sentence is that the data subject should be informed, that their data may be processed by third parties. So this is all what we’re trying to say in this. So the simpler we say it, the more clear that will be for everyone. That’s why references to documents and then specific parts of the document probably will create more confusion. So, in essence, the data subject must be informed that their data may be processed by third parties, full stop.

Then there’s a further request. Further sentences suggest that, upon request of the data subject, the data should be disclosed as soon as reasonably feasible, and so on and so on.

Can we entrust, based on this conversation, the staff to provide a simple formulation and go to the last bit of this, where the brackets need to be removed?

This is the last sentence of this paragraph. “Confidential requests can be disclosed to the data subject in cooperation with the requesting authority or (in brackets) in accordance with the data subject’s rights under applicable law.”

So we need to remove either the brackets or we need to remove one of the options – “and” or “or” – or we need to remove brackets and put a slash between “and” and “or.” So what’s the preferred course of action?

Chris is first. Then I have hands from Stephanie, Volker, Mar[c], and Brian. Chris, go ahead, please.

CHRIS LEWIS-EVANS: As I remember it, this “and” or “or” was dependent on who was the disclosing entity. I thought that was the homework that we had agreed to do earlier. So do you want to leave that as homework so we’re not just discussing it in the group for ages and we’ll come with a suggestion for tomorrow?

JANIS KARLKLINS: Can’t you make the suggestion now on the fly? Because now we know – no, no – who will be the disclosing entity. We know that the central gateway will do the recommendation [and] send the request and recommendation to the contracted party. The contracted party will make that examining request and [will]

validate the recommendation or reject the recommendation and formalize the reply. So this is the process that we agreed to in the morning.

CHRIS LEWIS-EVANS: Yeah. “And.”

JANIS KARLKLINS: “And.” Volker, are you in agreement?

VOLKER GREIMANN: We looked at this a little. We actually are in favor of “and/or.” So have both options in there. The requesting authority can stand on its head. If it violates the data subject’s right, we still have to disclose it. But we can still work with them [on] ways of how to do that. So “and/or” would probably be the best choice that incorporates both sides of the story.

JANIS KARLKLINS: Chris, can you live with “and/or”?

CHRIS LEWIS-EVANS: The only reason I don’t like the “or” is that it’s suggesting that you won’t cooperate with the people that have asked for it. All we’re asking for is cooperation, which is why I want to keep the “and” without the “or.”

JANIS KARLKLINS: Yes, Alan?

ALAN WOODS: Sorry. Again, noting that cooperation does not trump a legal right of the data subject, we just have to be very careful there. That's all I'm saying.

JANIS KARLKLINS: Chris?

CHRIS LEWIS-EVANS: And all we're asking for is cooperation. We might not make the request if it trumps the legal right. So we need cooperation before we're going to decide whether or not to go ahead. So, if take confidentiality and the answer is "We can disclose that. However, you're not going to get confidentiality," I then want to be able to make the decision on whether or not I want Alan to disclose it. I don't want Alan to disclose it and not make it confidential. So that's all we're asking for – cooperation – so we can make the decision on how we're going to proceed.

[That's what I said].

JANIS KARLKLINS: Okay. We have two options here: "and" only or "and/or." I would ask Chris and the CPH with a glass of wine tonight to come out with one, whatever it is. Okay? And that is noted tomorrow morning. We will get – sorry, Stephanie. We need to go on 56 now. 56.

Sorry. Yeah. Here, please. [inaudible]

MARIKA KONINGS: If you can also bear with us for, I think, the next half-hour because it'd really help staff if you can now review the remaining section in the report and indicate which ones you cannot live with so at least we can already make the updates that are non-controversial and everyone is fine with in the next version of the draft initial report.

I see Mark is waving his hand.

JANIS KARLKLINS: Mark?

MARK SVANCAREK: Hi. Sorry to do this, but I need to go back to the [third] sentence. My hand has actually been up for a while. "Data controllers must inform," or whatever language we come up with. That's a general obligation. This is in the Section 4 confidentiality of disclosure requests. I'm not sure that this language exists anywhere else in our report. It really needs to apply to all of these, not just the confidential ones. Thanks.

JANIS KARLKLINS: It seems to me that this is simply a heading of the subsection. Let me check with the full text of the recommendation.

CHRIS LEWIS-EVANS: I think Mark is right. When I looked through the thing, this was a safeguard that, for me, was very particular to the confidentiality side. I didn't find it anywhere else. So that's why I probably just jumbled it in there: to make sure we have the appropriate safeguards. If we extract that out and put that in the safeguard section, then I'm also happy, [he says], looking across at James.

DAN: Thanks. I was confused about this, too. It's in the section of the paper on Rec 8: Acceptable use policy. Then there's a section about an entity disclosing the data, which is strange wording. But we're living with that. Then it's down in confidentiality. But I do agree it does impose this kind of general obligation. The RA already requires registrars to inform data subjects of the intended recipients of the data. That's a 20-year-old requirement based on the old data protection directive. So registrars already have to inform the registrants of who's going to get their data. Then GDPR imposes new requirements. CPAA imposes new requirements.

This sentence here I worry when we get to [inaudible] we'll struggle to figure out what to do with that: if that's supposed to be a general rule applicable to all registrars. It's stating generally: data controllers of RDS data. We don't know who that is yet. Once you receive the data from the registrar, you become maybe a data controller of RDS data. How are you going to make this clear to the registrant.

So I think we probably meant to talk about registrars and not just any data controller who comes across RDS data. I agree it's a

more general obligation that shouldn't be buried here in this section. Thanks.

JANIS KARLKLINS: I'm just looking to the whole section here in the recommendations. This describes more broadly the obligations of contracted parties and SSAD. When you look to the full report on Page 18, you see that it suggests that contracted parties [and] SSAD must only disclose data requested by requester and must return current data and must process data in compliance with applicable law and must log requests and must [inaudible]. Last is that the data controllers of RDS data must make it clear to the data subject the types of entities/third parties which may process the data. So there is a logic that contracted parties [and] SSAD must do.

I thought that this confidentiality of disclosure requests is a subheading that needs to be basically deleted here and left only as a sequence of obligations or steps that need to be taken.

Please, Mark?

MARK SVANCAREK: I think, if you just break the line into two separate bullets … So there's one bullet that stands alone that says you must tell them who you're going to give the data to. The second one is regarding the confidentiality. Just turn those into two separate bullets and I think it works.

JANIS KARLKLINS: Okay. That's done already. So then we have a remaining … yes, Dan, please?

DAN: Sorry. So you said it's done. But to me, it's still unclear – the phrase "data controllers of RDS data." Did you fix that, too?

MARIKA KONINGS: Yeah. Basically now it's in line with the heading – "Contracted parties [and] SSAD must in a concise [inaudible] dah, dah, dah, dah." People can look at this language tomorrow and see as well the placements and if there's concern. But I think we removed that first part and made it a separate section.

DAN: All right. So, for implementation, the only thing was always ask for is to please tell us who must do what. Even here, how is the SSAD going to make it clear to data subjects anything? SSAD is not going to talk to data subjects. So are they out, too?

JANIS KARLKLINS: No. Here we simply need to look at that, now, when we have a model, we simply need to reconsider all these references and who does what. So, for the moment, this is when we did not know the model. We wrote the building block on a [new] policy and we said that contracted parties and SSAD should do A, B, C, and D. Now we need to see to whom to attribute, but your point is taken.

Yes?

DAN: Because this doesn't refer to that language. This says data controllers of RDS data, which is a different formulation.

JANIS KARLKLINS: Yeah.

MARIKA KONINGS: [It already moved].

DAN: Okay, thanks.

JANIS KARLKLINS: Now we're—

ALAN WOODS: Sorry.

JANIS KARLKLINS: Yes?

ALAN WOODS: Just jumping ahead in what this will be, I think we're going far too into the weeds of what we're going to say in these particular things. What's going to eventually have to happen is that all the contracted parties in our privacy policies will have to say, "Your

data may be released under the SSAD," link to SSAD privacy policy, and give an explanation of what that is and what instance … We're the ones that are going to be having that transparency on behalf of the SSAD placed on us. So that's what we're going to be looking at the future. It's not going to be down to the individual. It might be a certain person. It would be looked at [in] the terms of conditions of the SSAD itself. We will have to put that in as a separate thing in our privacy policies, without a doubt.

JANIS KARLKLINS: Brian?

BRIAN KING: Thanks, Janis. I was going to say that that's exactly what we should do: we should have policy language that says this language in these examples needs to be in the privacy policies or in the registration agreement or whatever it is. But I think we've known for a long time that we need to be very clear about that with the data subjects, with the registrants. So that's definitely something that we need to do.

JANIS KARLKLINS: Thomas and [Ben].

THOMAS RICKERT: That gives me the opportunity to get back to one of my favorite topics. In the joint controller agreement, you will allocate the responsibility of informing the data subjects that will be in there as

a task. I would predict that the registrars will be tasked with doing that because they are the ones holding the contact to the data subjects.

I would really hope that, instead of all registrants doing their own thing, one set of language that will be drafted be whoever will be used across the industry because, if somebody messes things up, everybody is going to be in breach.

JANIS KARLKLINS: Okay. Dan, please?

DAN: I don't want to derail us. I'm not sure I can agree with Alan. I don't know that there's going to be an SSAD privacy policy. I think we're envisioning SSAD to handle any registrant data right now. So I don't know why it would be involved. It's just that registrars or registries that are going to be giving data to requesters, which they already do today. Just a side note.

JANIS KARLKLINS: Marc Anderson?

MARC ANDERSON: I was looking for unmute there again. Dan is right. Looking at the Chameleon draft, that whole – where is my draft? – second section on CPH and SSAD is out of place in the acceptable use policy. It doesn't fit there. Here I'm looking at maybe [Berry], Marika, and Caitlin. It doesn't belong in Recommendation 9 at all

and probably should be its own recommendation. I think having it as part of Recommendation 9 is confusing and doesn't make sense. But that's not to say the stuff there in that second section – applicable to contracted parties and SSAD – has no value. It just doesn't apply to the acceptable use policy, which I think is part of why Dan is having heartburn over there: it doesn't.

So I think probably the easy solution there is to pull that out and make it its own recommendation.

JANIS KARLKLINS: Okay. We will consider that. Thank you for flagging this. Now it's 5:10. We sort of finished what we were planning for today, but we have about 20 minutes.

What I would like to ask you to do in these 20 minutes, in 18 of them, is to look through the query policy, terms of use, and logging [,] implementation guidance.

THOMAS RICKERT: I'm sorry. Just a quick response to your point, Dan. The SSAD is likely not going to be a separate legal entity. But the SSAD as such will handle a ton of personal data for the requester. It will do the logging that has IP addresses in it. So I think we will need to come up with a very comprehensive document explaining all that just so that it doesn't get forgotten.

JANIS KARLKLINS: Yes, Marc?

MARC ANDERSON: That is covered in the Chameleon draft. There is a section that does cover that. It's the privacy policy section for how the data collected by the SSAD system will be handled. So you're right, but it's already accounted for in the Chameleon draft.

JANIS KARLKLINS: Thank you. I would now give you your freedom for the next 15 minutes. Please look through those sections that I mentioned: query policy, terms of use, logging [,] implementation guidance. In the remaining two minutes after the break, you will indicate which paragraphs you want to talk about tomorrow.

UNIDENTIFIED FEMALE: Cannot live with?

JANIS KARLKLINS: Yeah. So the query policy, terms of use, logging [,] implementation guidance.

ALAN GREENBERG: Some of thus have already done that. Can we have an update if there's anything that needs to be updated? In other words, some of us are already finished. Do we have to wait for ten minutes?

UNIDENTIFIED MALE: Some of us were finished an hour ago.

UNIDENTIFIED MALE: Logistics-wise for dinner tonight, you'll basically need to start leaving from the hotel around 6:30. Try to coordinate with Ubers as much as possible to get over there. It'll take about 20 minutes with traffic. So it's at the Wallace. I've been there before. It's pretty darn good. We're very short. We paid for 40 heads, and only 27 of you are showing up. So I'm going to try to negotiate better wines, but we'll see.

The last-[day] thing is that the badges that you got today please leave on the table. Do not take them with you.

UNIDENTIFIED MALE: [inaudible]

UNIDENITIFIED MALE: This table.

JANIS KARLKLINS: Also, for those of you who want to join me in walking to the restaurant from here, please feel free to do it. It's a 1 hour 20 minute walk/6 kilometers. After sitting all day, it is good exercise.

UNIDENTIFIED MALE: [I'm not feeling it].

UNIDENTIFIED MALE: Sponsored by the American Heart Association.

MARIKA KONINGS: Alan, are there any on your list?

ALAN: No.

MARIKA KONINGS: No issues. Great. Okay, good. Homework. No leaving.

JANIS KARLKLINS: Those who do not issues may leave, but otherwise we're breaking now to consider the last sections I indicated. We will resume whenever you're back in the room but not later than 5:25.

I understand that there have been already some communication. If I may ask Marika to communicate who has already told the numbers.

MARIKA KONINGS: I have numbers from the GAC and the BC and IPC who all flagged #63.

UNIDENTIFIED SPEAKERS: [inaudible] 66

UNIDENTIFIED FEMALE: 66?

MARIKA KONINGS: Okay.

UNIDENTIFIED MALE: 62.

MARIKA KONINGS: 66? I did just speak to Mar[c] about that one and he thought it was no longer—

UNIDENTIFIED MALE: 66?

MARIKA KONINGS: Yeah. So—

UNIDENTIFIED MALE: [inaudible]

JANIS KARLKLINS: So then the only issue is with 63?

MARIKA KONINGS: No. Registry—

UNIDENTIFIED SPEAKERS: [inaudible]

UNIDENTIFIED FEMALE: 68? 62?

THOMAS RICKERT: And 63.

JANIS KARLKLINS: Yeah. 63 is on the list.

MARIKA KONINGS: Yeah.

UNIDENTIFIED MALE: [inaudible]

MARIKA KONINGS: Sorry. Which ones?

UNIDENTIFIED MALE: You can send multiple [requests].

JANIS KARLKLINS: You cannot live with that. Franck, you cannot—

FRANK JOURNOUD: We're good.

MARIKA KONINGS: [63?] Okay. 57 yes or no?

UNIDENTIFIED MALES: 57. Yeah, 57 because [inaudible].

MARIKA KONINGS: So I think 57 is one of those that we actually did discuss extensively, so it would be helpful, if you want to talk about that one, to come with new information during tomorrow's discussion on why that should be reopened.

UNIDENTIFIED MALE: Can you scroll?

MARIKA KONINGS: Oh, sorry.

UNIDENTIFIED MALE: [inaudible]

MARIKA KONINGS: Okay. Off the list.

UNIDENTIFIED MALE: Okay.

JANIS KARLKLINS: So we're taking 57 off the list.

UNIDENTIFIED MALE: [Perfect].

JANIS KARLKLINS: Which leaves us with having a conversation about 58, 62, and 63.

UNIDENTIFIED MALE: [inaudible]

MARIKA KONINGS: [inaudible]

UNIDENTIFIED SPEAKERS: [inaudible]

JANIS KARLKLINS: So tomorrow morning we will take those three points. After that, we will go to the purposes. So we will take those three points in the morning and then we will go to the purposes discussion.

UNIDENTIFIED MALE: [inaudible]

MARIKA KONINGS: If I could add something there, I think, for purposes, there are two proposals on the table. One is the staff language in the report. I think the other one is the BC language. So it may be helpful for people to come prepared to indicate why they cannot live with either one of the proposals for that conversation.

JANIS KARLKLINS: Thank you. Thank you for active participation and a constructive approach. This meeting stands adjourned.

[END OF TRANSCRIPTION]