ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 1-AM
Monday, 09 September 2019 at 15:30 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/6oECBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

JANIS KARKLINS: And the comments that have been received until yesterday now have been Introduced in 0.1 version of the draft that Marika sent to the team yesterday around 10:30. That document would be the one we would use for our meeting these three days.

Also, agenda has been circulated, and to my knowledge, no objections have been received, therefore we will follow that agenda as suggested. The only difference is that as Milton suggested in our call, we would not strive to follow exact allocated times, but we will take as much time as needed to talk about issues in the sequence that is proposed.

Of course, it will not be eternal. At one point, we need to cut off, and probably, that will be when we will start going in circles on certain issues. But in principle, we will follow the sequence rather than timetable.

That said, I will now ask Gina to do a little bit of introduction from her side.

GINA BARTLETT: Good morning, everyone. My name is Gina Bartlett from the Consensus Building Institute, and I've said hello to many of you, and there's a few people I haven't yet met, so I look forward to speaking with you on the break.

My job is to complement Janis' work as the chair and serve as your impartial facilitator and mediator helping you work through your agenda and review toward the outcomes that you've identified that you'd like to work on.

Before we jump into some of the mechanics of how we're going to work together for the face-to-face, we wanted to go around and invite everyone to please introduce themselves. I've been restricted from having you do something funny, so we'll just stick with your name and your role. Thank you.

JAMES BLADEL: I'm James Bladel from a registrar and I'm incapable of being funny.

MATT SERLIN: My name is Matt Serlin for the Registrar Stakeholder Group. I am capable of being funny, usually at James' expense, so I'll spare them for now.

VOLKER GREIMANN: Hi. My name is Volker Greimann. I'm German, and therefore the humor of myself is debatable. I'm also here for the registrars.

MARC ANDERSON: Good morning, everyone. I'm Marc Anderson from the registries, and I have no idea how to follow any of that. So I'm clearly not as funny as my registrar colleagues.

MATTHEW CROSSMAN: [I'm from the registries, and I echo in rooms.] Matthew Crossman from the registries. I'm new so please be gentle.

BRIAN KING: I'm Brian King from MarkMonitor. I'm here for IPC.

ALEX DEACON: I'm Alex Deacon, also with the IPC.

THOMAS RICKERT: Thomas Rickert, ISPCP.

FIONA ASONGA: Fiona Asonga, ISPCP.

BEN BUTLER: Ben Butler, SSAC.

GREG AARON: Greg Aaron, SSAC.

SHLEY HIEINEMAN: Ashley Heineman, GAC.

GEORGIOS TSELENTIS: Georgios Tselentis, GAC.

CHRIS LEWIS-EVANS: Chris Lewis-Evans, GAC.

LEÓN SANCHEZ: I'm León Sanchez, ICANN board, and I'm the Mexican that [complains the joke.]

CHRIS DISSPAIN. Chris Disspain, ICANN board.

DAN HALLORAN: Good morning. Dan Halloran, ICANN Org liaison for Legal, and welcome everybody to Los Angeles. Sorry, I meant to welcome you last night. I was tied up with family stuff, and this morning, I'm here so I had to bring my son to school [inaudible] so sorry, I missed the [inaudible]. But welcome, everybody. Good to see you again.

TRANG NGUYEN: Trang Nguyen, ICANN Org liaison from GDD.

MILTON MUELLER: Milton Mueller from the Noncommercial Stakeholder Group.

AYDEN FÉRDELINE. Hi. Ayden Férdeline with the Noncommercial Stakeholder Group.

JULF HELSINGIUS: And Julf Helsingius, same group.

STEFAN FILIPOVIC: Stefan Filipovic, NCSG.

HADIA ELMINIAWI: Hadia Elminiawi with the At-Large Advisory Committee.

ALAN GREENBERG. Alan Greenberg, ALAC.

MARK SVANCAREK: Mark Svancarek, Business Constituency, and my role is [croissant.]

MARGIE MILAM: Margie Milam with the Business Constituency.

BERRY COBB: Berry Cobb, consultant with the policy team, just glad to be here and here to help the team in any way that I can.

CAITLIN TUBERGEN: Caitlin Tubergen, ICANN Org.

MARIKA KONINGS: Marika Konings, ICANN Org.

GINA BARTLETT: And do we have anyone online yet, Terri? No remote? We also have some alternate observers in the room. Would you like to introduce yourselves, please?

Great. Thank you, everyone. So the next thing we wanted to do was just to review some working agreements for our time together, and I think we were going to start with Caitlin. Caitlin was going to walk us through the EPDP working guidelines, I forgot what they're called exactly. Rules of engagement, I think.

CAITLIN TUBERGEN: Thanks, Gina. I believe Terri is going to assist us in putting this up on the screen. But what you're now seeing on the screen is the EPDP team statement of participation, and some of you probably read over this last July before you agreed to become a member of the EPDP team. So we just wanted to put this up as a friendly reminder that everyone in the team agreed to adhere to these guidelines.

I won't go through and read them, but I just wanted to note that all of the members at the table agreed to be civil to one another, to be respectful of one another, to allow all the stakeholders to be heard, and to not purposely disrupt conversations and to strive to build consensus where possible. Thank you.

GINA BARTLETT: I'm going to just add on a few additional very pragmatic things. We're asking that all interventions – that is the same thing as making comments – be by group as much as possible, and so to that end, we will periodically say, "Take five minutes and talk within your caucus," but you also can ask for time to consult with your group and just call for a caucus in order to be able to work through and determine how your group would like to engage and your thoughts on a particular matter. Alright?

The other thing is we are going to queue with the name plates. I know that that's not always popular with everyone here. And then staff are going to help Janis and me keep track of the order of the queue and bring in the remote participants and add them into the queue.

However, I do want to reserve the ability, if we are trying to negotiate an outcome and come to closure on an issue, we may ask you, if you have a new topic, to hold off for a few minutes and pick up the people in the queue who are trying to help bring us to closure. And then when we're done with that, we will go to the new thread or new topic sequence.

We've done that quite a bit in the past, and I think it just helps bring things to closure rather than having so many different conversations going on. Is there any concerns or questions about that approach? We will just do it when it happens. Yeah, Milton?

MILTON MUELLER: You mentioned interventions by groups. That means stakeholder groups and ACs, right?

GINA BARTLETT: Yes. Stakeholder groups? Oh, I'm sorry, can you clarify?

JANIS KARKLINS: Milton, you know the answer.

MILTON MUELLER: Yeah, stakeholder groups and ACs.

JANIS KARKLINS: We have groups here that are determined by the charter of the team. So when we're speaking about groups, we're speaking in the meaning of groups of [teams.]

MILTON MUELLER: Well, I'd read the charter, it's not what I saw in it. But we can refer to that if you want.

GINA BARTLETT: Yeah, I think I understand it's difficult to be able to negotiate as a group, but we are going to ask you to please – and we've intentionally sat you together so that you can talk with one another during the caucuses. So we really are going to strive to operate by group.

We're doing that primarily because that is the nature of the long-term agreement that you're able to and need to reach, and secondly, because we always struggle with time. And so we appreciate the uniqueness of each person's voice. We know you all have a lot to contribute, but we also recognize that we have an ongoing conversation with each of your groups, and your charge is to represent the interest of your group. So we're going to strive for that.

JANIS KARKLINS: So yeah, I think once we will start going through topics, there will be natural kind of dynamic in the room, so we will follow, and what Gina said, that probably should be seen as a preference rather than as a fundamental rule. So simply to have conversation going and that we're reaching consensus on some issues, if that's possible here.

GINA BARTLETT: The other thing we wanted to touch on was the chat. The chat will be open, but we really want to encourage folks – the reason that we are here together and have spent all of this time and resources to come together is to have a conversation in the room, so we would strongly encourage you to have the conversation in the room rather than in the chat.

We learned kind of the hard way that the chat is a very useful tool for answering quick questions and clarifications, but we really want to encourage you all to please have the substantive conversation in the room as much as possible.

The other thing we wanted to just touch on is I think we have a few meeting logistics like room logistics. Terri, didn't you want to go over a few things from a meeting logistics [perspective] or anything, like in and out, exit?

TERRI AGNEW: So we are just going to ask that you stay in the main hallway to go to the restroom and not wander off to other areas. If you do need a private area for a telephone call, there's a couple of what they call pods that I can take you to. There's one on this floor and one on the floor above that’s a little bit bigger. Or if you need to go to the break room or something, if you could just find staff to kind of help walk you around the office and stuff, we would appreciate it. back to you, Gina.

GINA BARTLETT: So that’s all the housekeeping. Is there anything else anyone wants to bring up or raise? Okay, if not, then I think Janis is going to walk us through the agenda. Sorry, James.

JAMES BLADEL: Sorry, just a note that some of the remote folks are saying that the audio is very faint. So can we just ask folks to make sure you’ve put the microphone directly in your face? And then they said they’ve got the volume cranked up very loudly and they're still having difficulty hearing some folks.

JANIS KARKLINS: Yeah. So we will do our best. I don't know how to speak with a microphone in your mouth, but I will try. So the idea of these three days is to see how far we can get in developing the draft 1.0 based on our agreement that the document in front of us would be used as a basis for our activities during this week.

So we have today a scheduled meeting with the CEO and Strawberry team. That will probably help us clarify some burning questions that we formulated together in the letter, in the e-mail that I sent on behalf of the team to CEO and to Strawberry team, but also, we will be able to ask whatever questions are in our mind during that conversation.

So prior to that, we will spend some time talking about and reconfirming the overall understanding of architecture of the system. I think that that is important, that we're still on the same page going further.

And after conversation with the CEO and Strawberry team reps, we will sort of take note or take stock where we are, and how information that we will receive fit in our joint reflection on the policy proposal that we're working on.

After initial conversation about architecture and questions that we may ask to CEO on top of those that we have already formulated and submitted, we will start working on building blocks, and then working on building blocks is the essential part of our activities throughout today and tomorrow.

We asked the team to send in priorities how you see we need to address issues. Ultimately, we need to talk about all of them, but simply using idea of the survey was to identify those topics that you think we need to address as a priority during the face-to-face meeting, and so identified topics now are reflected in the agenda.

We will start with the accreditation and associated conversation about user groups or user categories, and here we received yesterday a note from Milton that outlined number of ideas and options, and I will ask Milton when time will come to introduce his memo to all of us to kickstart discussion, and then depending on time and then how swiftly we will progress and fine tune our understanding, we will go to another topic that is on purposes and legal bases, but also issues team identified as top priority for our conversation.

So I doubt that we will be able to do something more, but if so, then we will see whether there are any other issues we could address today. So this is a preliminary program for our conversation today, and I hope that is acceptable, unless someone is wishing to take the floor now for any comments or reaction. Please, Alex.

ALEX DEACON: Yeah. Hi. Not too long ago, I sent a PowerPoint with some of my thoughts about accreditation. I guess better late than never. But if we have some time, I'd like to walk the team through that in the hopes that we could agree on some type of framework at least to have the discussion about accreditation moving forward. Thanks.

JANIS KARKLINS: Yeah. Certainly. Sorry, I have not seen it I have not opened computer yet since 8:00 AM. But yeah, no, certainly, and thank you very much for sending [that.] And actually, I'd like to encourage team members to think, to look which topics need to be further developed, and there are many of them that we have not either touched at all or we have touched only slightly. And in the style of Milton's memo or Alex's thoughts, just drop your proposals that potentially could help us in kickstarting that discussion.

So if that is okay – yes, Thomas, please.

THOMAS RICKERT: Yeah, I think this will likely fit in nicely with the discussion on accreditation, but my observation is – and I didn't bring this up as a separate proposal for discussion because I think it's embedded in there, but talking to various people in this room and outside, I guess we're still not aligned on what the projected outcome of this is going to be, and I think we might have as many views on how this all can be operationalized as we have brains around this table.

So maybe we can seize the opportunity, hopefully, even before Göran is coming in and when we're discussing Milton's suggestion on how this can be operationalized and who would actually do what and how the liabilities and responsibilities could be distributed.

So I think it's not a separate discussion, but I'm just suggesting that we take a few minutes to touch upon that.

JANIS KARKLINS: Yeah. Certainly, and actually, I think, Thomas, that that more belongs to the systemic discussion that I'm planning to engage now as soon as we finish this part of the conversation, that then we can exchange views and see whether our understanding is fully aligned or closely aligned, or not aligned at all. I think that that is where that fits in my [view.]

So with this, maybe also from my part, one request. Try during these three days to put yourself in the mindset of while stating your long-standing views and positions, listen to others and try to adjust your positions in light of positions of others, because that is the only way how we can really progress in our discussions and narrow the gaps that we have.

If we will camp on our positions that have been expressed two, three years ago and without giving up anything, then we will be at the end of the meeting exactly where we are now. So as a result, please use these three days also to listen others, try to adjust your thinking in light of what you hear, and also what you see, because body language also is important.

And most likely approach should be not whether I can accept that but whether I can live with that. I think that that would be the right way of looking at things, because we are not working towards, let’s say, ideal outcome. We’re working towards consensual outcome and consensus is never ideal. Consensus is always crippled, and as a result, everyone needs to be able to live with it and be equally unhappy. So that would be my request and suggestion.

So with this, I will now try to [inaudible]. Now it's working. So we're talking about a reasonably simple model. We're talking about something that looks like a hamburger. ICANN these days is very much in food titling, and we will hear today Strawberry team, and we will confront Strawberry team with the Hamburger team.

And of course, Hamburger is made of essentially three parts. One is what is on the top, what is on the bottom, and then something that is in the middle. And essentially, all three parts are equally important, but some things may be also outside this, like for instance wrapping paper that we put around a hamburger not to make our fingers too dirty.

So more seriously, when we're thinking how a system works, we have a request coming from somebody, somebody identified as individual or somebody identified as a group, or categorized as a group.

Then we have those who possess information, that is registries, registrars, and those who potentially, if all stars are aligned, will disclose requested information to requestor.

And then there is this middle part that ensures that request goes through and answer also goes back.

So the [demand side] is built from certain building blocks. They may be separate, they may be intimately linked, but certainly all of them are necessary to determine how request is formulated, who does it, how, whether requestor is legitimate or not so legitimate, is known or not known and so on.

So in that respect, we have a number of building blocks that are outlined in the paper. So I may not remember all of them, but for instance, how a request is formulated, accreditation and associated categorization for the purpose of accreditation, I would argue. Then some other elements that are linked with the formulation of a request.

Then it comes to this interface part, and in theory, we can think of a number of options here. One option is that there is one gateway where all requests come. In theory, there may be multiple gateways where request come, depending on the nature of the request and whom that request may be addressed.

Then what happens in this intermediary? There might be just a simple check whether requestor is legitimate or not. In other words, the check of credentials issued by accrediting authority. Equally, here may be also some kind of determination made on the validity of the request. And then whatever is done here goes down to the supply side, to registries, registrars, where again certain actions are performed based on our building blocks that we have. And a reply is given if all characteristics or conditions are met, and that goes back to requestor.

So I think that the discussion with CEO today most likely should turn on this intermediary phase. Understanding what role ICANN would play in this sort of processing of information, whether at all, any. We can think that at this level, ICANN acts only as the central gateway and verifies credentials, and does nothing more. So all the balancing act that we’re talking about can be done at the registry/registrar level. That’s one option.

Equally, we can think of option where the determination is done at this level, at the gateway, and nature of the request that is sent down to registry or registrar is different.

In the first case, if no determination made here, the requestors just send ”This is a request coming from valid source, please do determination and decide whether you provide answer or not.” If the determination is made at this level, then the request is, “This is the request, please send this information because we did all the checks.” So that’s the one option that we could think of.

Though I must say there might be a third option that we could also consider and contemplate, that determination is not done at the gateway but the determination is done somewhere else. Not impossible, but hard to imagine. But maybe it is something we may also consider. In other words, the determination is done by external entity as a theoretical model, nothing more. So these are things that we need to talk through and see where we are.

So now the big question is the liability, how liability is divided among those actors involved in the processing. And then here of course, extremely important is answer that will be given by CEO, what liability sharing we can expect, if at all, and whether there might be an option where all liability is outsourced and to outside organization that makes all the determinations. So that’s again a theoretical model is probably worth contemplating.

So this is in essence the proposed architecture which is built in zero draft and commented. Probably also it’s worth mentioning that building blocks can be discussed independently from discussion of what happens here in this intermediary phase, because they will be the same in different options that we may contemplate as we're processing information here.

So therefore, if we will not get on the same page on one model as a result of today's conversation with CEO, that we could then continue working. We still can work on every building block, and in parallel, continue contemplating on, let's say, structural issues, architectural issues, how the system will function if we all can agree on that.

So that is the way how we thought and built the proposal of zero draft.

GINA BARTLETT: [inaudible].

JANIS KARKLINS: Yeah, no, I already explained.

GINA BARTLETT: [inaudible].

JANIS KARKLINS: And the question at this stage is, are we in general, in principle, in agreement with this type of approach that we can continue working? And I see Milton's flag is up.

GINA BARTLETT: [inaudible].

JANIS KARKLINS: No, let's, for the moment, collect first reactions that we have. I have Milton, Alan, Thomas, James, Georgios in that order for the moment.

MILTON MUELLER: Thank you, Janis. I think in general, it's going to be more efficient to let people from groups spontaneously react and not have to confer before everybody speaks. I don't think that model's going to work.

But anyway, I like the hamburger. Big fan of hamburgers myself. But I don't see a good correspondence between the hamburger and the zero draft in every respect. In other words, I don't know where for example user groups fit into the hamburger model.

And in fact, I think one of the things I like about the hamburger model is it has no user groups and see no need for them. So there's the little dots, the sesame seeds and the ... Yeah, so as long as we can question the necessity of different parts of the building blocks, I think the hamburger's a good overall summary, so I would leave it at that going forward.

JANIS KARKLINS: Thank you. Alan's next.

ALAN GREENBERG: Thank you very much. Just one comment, or a few comments just on my assumptions. I presume there also a path bypassing the middle of the hamburger, just going from one bun to another, because no one's going to prevent anyone from making requests. It's not our concern, but it's there also.

You referred to the hamburger in the middle as being ICANN, or it could be outsourced completely. I've always worked on the assumption that it's not necessarily a uniform blob of hamburger, but it might well be made up of many different parts, some of which ICANN might run itself, some of which ICANN might outsource, or other services such as an accreditation group for lawyers or whatever might be a resource it draws upon to put it in.

So it's not an amorphous blob, but it might well be composed of a whole bunch of building blocks, each of which are managed differently and under appropriate contract. That's my assumption. If that's not right, then I think we're talking at odds with each other.

JANIS KARKLINS: Look, I think that nothing is decided. What is sort of proposed, that there might be accreditation. Might be. Then we need to work out what that would entail, how that could be done, what principles we need to build an accreditation system. That needs to be determined here.

So then, who will do that? That's another question that also we may want to talk, we may let implementation team to consider. So everything is up for conversation.

ALAN GREENBERG: I just want to make sure that it wasn't an amorphous blob, that what you're talking about is still on the table. Thank you.

JANIS KARKLINS: No, look, everything is on the table until everything is agreed. So that's the, again, basic rule. What we're trying to do is trying to stabilize some ideas that we do not reverse back after three, four months saying, "Hey, I thought that's wrong."

No. If we agree to stabilize something, then we do not revisit it. We take it as agreement. And then slowly, we're progressing in a certain direction. Thomas.

THOMAS RICKERT: Janis, I agree with everything that you said. I think that the middle part, the patty, is a little bit too opaque as to [inaudible] with real life and roles. So if you would indulge, can I use a few square centimeters on the whiteboard to share with you how I think it can be made work?

JANIS KARKLINS: Yes, please.

THOMAS RICKERT: And I promise not to introduce more food analogies, nor will I try to be funny.

JANIS KARKLINS: Please do.

THOMAS RICKERT: Because I think there is an awful lot of confusion around the question of validation versus accreditation, and then automated processing of requests versus semi-automated responses to requests, and the liability questions relating to that.

And I think that – and you can criticize me after I've shared with you my view, but one way it could be envisaged is this. Let's just assume for a second we have registries, we have registrars, and we have ICANN. Some say that these three are joint controllers, others say that they are independent controllers.

So let's just assume for a second they were joint controllers. And I'm mentioning this explicitly because when the GDPR was drafted, this notion of joint controllers was introduced for scenarios where it is difficult for the data subject to determine who does what.

Let's say you're buying something online, you don't know who's going to deliver the goods to you, you don't know who's going to do the billing, you don't know who's feeding the ads, and therefore you can go to any of them and exercise your rights. So that's the idea behind it. And I think that it might be equally difficult for registrants to know who's behind all this. Registries, registrars, ICANN, EBERO, escrow agents and all that.

So we can still disentangle that later on, but let's just assume these were joint controllers. Then within this concept, you can allocated functional responsibilities. That's what you would do in a joint controller agreement.

I think there's agreement in this room that ICANN would be the entity – and I know that Göran and the Strawberry team are working on this – to make sure that ICANN plays a particular role when it comes to the disclosure mechanism. So they're basically doing this on behalf of the joint controller.

How would that then work? ICANN, let's put it here then, would establish such system, and they would – and this is where your burger would come in again – then if our group chooses to have an accreditation, let's say for law enforcement authorities so that you do know that, let's say, a request coming from a Hotmail address – and I do know that some law enforcement authorities are still using Hotmail addresses – that these are legit law enforcement officers.

So let's say Interpol was doing the accreditation. Probably, they don't, but let's just assume that. And ICANN could task Interpol with accrediting certain user groups, so could potentially WIPO, just for illustration purposes.

But they would be doing that on their behalf. So then you would have within this the demand side where you would have eligible parties that can file requests, either based on an accreditation which would then go through such third parties, or they can just go there and be validated in one way or another. Let's say if a user wants to know what domain names are registered for them, if they exercise their rights, then probably validation that the individual is actually the individual is good enough and you don't need a full-blown accreditation for that.

But they would still be doing that on behalf of ICANN. And when it comes to liability for all that, these would be jointly and severally liable. That's wah the law says. But internally, they could indemnify each other for who did something wrong. You can cover that there.

Also, the joint and several responsibility would only apply for external claims that are raised by data subjects. If the authorities want to sanction – which is probably the biggest risk – they would go after the wrongdoer anyway.

So ICANN could then take care of the accreditation part, either do it themselves or have accreditation agents such as these do it for them, and then you would have the requestors, and then maybe this thing would be the black box where things are being processed, either based on an accreditation where requestors could then file requests based on accreditation or any other mechanism.

Then the other thing is I guess we need to be very clear that within this black box, within the burger patty, you have different roots. So my hope was when suggesting the first use case, that this would be, the IP thing would be an avenue for automated processing. So if you have an accredited party, let's say it were accredited by WIPO, and if the criteria are met which we establish in the use case or then in the policy, then there would be a request, there would be some checks, and then the data would be supplied, as in your visual.

That would be automated, and the requestor would need to pay an accreditation fee, and they would likely need to pay some other use-based fee. And part of that I think could go into a risk fund, out of which if something goes wrong, these parties could be compensated so that you build some financial safety net into the entire system.

Hopefully we're going to be able to determine as many cases for automated processing as possible, because I guess that's what we're trying to achieve here, that for high volumes of requests, we spare the entire industry the manual intervention. Therefore, we need to make sure that we have prefabricated balancing tests which need to be far more detailed than what we have in the use cases at the moment so that if a certain type of request comes in, we do know that we have balanced the rights of the data subjects concerned with the interests of the requestor, and therefore those clear-cut cases, you can give an automated response. Right?

And then we need to make a clear cut, and at the moment, we are conflating these two areas. We would have different types of requests that either would not qualify for automated processing, or not for the SSAD as such. And they need to go into, let's say, this [work bucket] A, they'd need to go into bucket B where there's some manual intervention. The accreditation can take place where accreditation fits, but then you would have manual assessment for other use cases, and there would be different rules. There would be a balancing test on a case-by-case basis, and what data is going to be revealed will be dealt with on a case-by-case basis.

And that, again, could be done by a third party, let's say an external evaluator hired by ICANN as they do for their financial vetting for new gTLD applicants. ICANN doesn't do any of these things by themselves. But I guess I know that this looks extremely ugly, but I think getting clarity on what the parties would be and keeping the discussion separate would at least help me a great deal.

And I think we should be focusing on that to have the clear use cases that can be worked on automatically in the first place, because that's likely where the highest volume of requests is going to be produced, then we're going to have a different bucket for manual processing.

JANIS KARKLINS: Yeah. Thank you, Thomas. I think that's not much different. There are nuances of the overall proposed architecture, as I see. But the next was James followed by Georgios.

JAMES BLADEL: Thanks, Janis. Thanks, everyone. Thomas raised a number of the points that I wanted to get into the discussion as part of a reaction. I think that just a couple of comments. The first one is that I think this idea that the decision making is attached to the liability, so wherever the liability lands for this burger, the decision lands as well. We can't separate those where folks are essentially assuming liability for decisions and actions made by others. I think that's a noncontroversial statement.

And then also, and I think Thomas touched on at the end as well, is that we need to at some point – and hopefully that opportunity is now – start thinking about the economics of how this system is going to work and who’s going to pay for it. This is a significant undertaking that’s something that’s never been built before that I can say from even a large provider, there's absolutely no space on the development roadmap or any funds or schedule from engineering time devoted towards this.

So where’s that going to land? And then once it’s up and running, who’s going to maintain it? This is a significant system. I like the idea of indemnification. It’s something that we've talked about. But I think we also have the blood from a turnip problem of the potential fines being completely asymmetrical to any amount of risk funds that we could possibly accumulate here.

So perhaps maybe instead you are buying insurance. And for that, I think we also need to put our friends from the GAC and our government friends on notice here that your contribution can't just be what you want from the system. You have to help us sell it to your colleagues who are going to come after us once it’s up and running. That is, I believe, also a natural role for our colleagues from the GAC. It’s not just to lay out your requests but also tell us what you're going to do to help us run interference and champion this model with some of your colleagues who may need some convincing.

So those were just some of the comments I think that I wanted to introduce into this, but mostly, I think the biggest omission is the economic discussion and where all of that lands. Thanks.

JANIS KARKLINS: Yeah. Economic is on the agenda. The financial model, we need to start thinking and actually, in Thomas' presentation, he mentioned a few elements, how a system could be funded. But if there is a wish by somebody to make maybe more than two bullets on the topic, please feel free and circulate that to the rest of the group, simply to stimulate thinking about it. Because one thing is to build a system, to introduce the system, and then to maintain the system and run the system. So there are a number of elements involved that everything will cost money.

Georgios is next followed by Marc, and then [inaudible].

GEORGIOS TSELENTIS: Thank you. I like the idea, as we move to any type of model, that we are talking concrete. So in this sense, hamburger is welcome because it's a model that we can start to visualize what is going to happen, but what you did present, Janis, is the quick and dirty, high-level view, then we jumped to what Thomas was saying, and I wanted to put things somewhere in the middle.

If we talk with GDPR jargon, we're talking about processing activity, so the big is disclosure, and then we break up those to specific sub-processes. And for each sub-process, we have the actors and we have the liability that goes with it.

So in any model that we're going to discuss, I think the more we get to the details, the more we have to be clear who are the actors and what are those processing activities, and another parameter that I think should be on the table is when we are talking about personal data, we are talking about flows of data that are crossing jurisdictions, and this flow of data has an impact on how this liability will be judged at he end of the day.

So in the initial model you presented, Janis, there were several variables, several options that we could have there, and if we go to all those options, we can see that data and not necessarily [go the parts of data are changing, can change] dramatically.

So in the discussions, I think we need to clarify also when we are talking about centralized gateway. We're talking centralized gateway about tokens that are deciding where the data will flow, are we talking about data that are going to flow through a gateway, where this gateway will be, where is the host of this? So all these are parameters that need to be defined.

Then we can go even to all these details that I agree with Thomas that need to be spelled out. There are several ideas on the table, and each one of those impacts exactly the two things that I said; the processing activity and the responsible party for this processing activity, which from that stems the liability, and the data that needs to flow and from where to where.

JANIS KARKLINS: Yeah. I think that the assumption which is kind of logical is that liability lies with the entity that makes the determination, makes the decision whether to disclose or not disclose data, right?

And then the big question is where that determination is done. So today, the determination is done at the registry/registrar level. Since the stakes are high, in principle, everything is sort of hidden, and no disclosure. No disclosure, no risk.

So, is that system sustainable from, let's say, the Internet stability, security, resiliency point of view? Probably not really. So hence, this is why we're here. We're talking about it. And we need to find the reasonable solution to make sure that some data is disclosed when it's needed, when it's lawful, and then who does it? And then how the liability is spread across the system.

And I mentioned one of the options is to think whether the determination could be done at the gate by ICANN. Let's be clear, because that's most logical thing, or that may be done by somebody outside the ICANN remit with also a division of liability with that. So that's kind of a theoretical option.

Thomas mentioned that organizations like Interpol or WIPO could do accreditation. Question is whether we can think of that they would do also determination. That's the question to contemplate. Maybe, maybe not. We don't know. We're not yet there.

Marc Anderson, then Ashley followed by Hadia.

MARC ANDERSON. Thanks, Janis. Thanks for presenting the hamburger model there. I think, when I was listening to you sort of tee up the conversations, what I liked about what you're saying is the way you teed up the question that we have to consider here and the answers that we're trying to define. I thought that from that perspective, you did a good job laying that out.

There's a lot of fundamental building blocks that we have to sort of find answers for before we can get to that first goal you listed as agreeing on what the architecture of this model would look like, and hopefully, before I got on the plane to come out here, I [listened to the TSG] model, sort of refamiliarized myself with that.

A lot of the purpose for that [TSG] model is to find out what is possible under GDPR, some of those very same questions that you were asking at the start. And in fact, section eight of the CSG model has four different action models, some of which are very similar to the different scenarios that you were describing.

So I'm really hopeful that when we meet with Göran and the Strawberry team later today, we’ll get some more clarity on what is possible with conversations they've been having and what's come out of the [TSG] model since then. I think we've had some really good interventions so far, people laying out some really good food for thought I guess as we delve into these models. But I really thought you laid out some of the different possibilities, lots of different possibilities for how the patty between the buns there can be developed, but you really, I thought, hit the nail on the head as far as what I thought the questions we’re trying to answer here. So thank you for that.

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

ASHLEY HEINEMAN: Thanks. Yes. I think this illustration and conversation is really timely and necessary. I think we've been dancing around this hamburger for quite some time not even realizing it, so I think just concretely putting it before us is really helpful.

I think it's probably a bit premature to go with the level of detail that Thomas went into, but it did raise, I think, some important questions that we might still need to consider, and I'm certainly not the expert on this, but there seems to be this assumption that accreditation is also the responsibility of ICANN.

I'm not sure that's the case. We haven't really gotten to the point where we're spreading liability around a bit. It may not make everybody happy here, but at some point the liability should not sit squarely on ICANN and the contracted parties' shoulders, and at some point, the liability needs to be recognized on the side of those requesting the data.

So just some things to keep in mind, that we shouldn't jump to conclusions, that if we are able to get to a point of having user groups that are represented by an [accrediting] body, that that is liability that's brought within this construct, and perhaps that's something that we can recognize but is ultimately left to the development of parties outside this group. Thanks.

JANIS KARKLINS: Thank you. I think on that level, we have already agreement, and that is reflected in the policy principle, at least one of them, that also the requesting side bears liability for its actions, and I think that that is our fundamental understanding that also we need to always keep in mind.

Hadia followed by Greg.

HADIA ELMINIAWI: I actually like the hamburger model, and I would put in the middle – so we have in the buns the demands, and that could be user groups or denial users, and then in the middle, we have slots which would typically be authentication, accreditation, and decision making, or decision making could be put into two.

Some of our decisions, whether it's going to be part of three or two, depend on the risk associated with the determination. For example, if we know in advance that having an entity other than the contracted parties making the decision-making would reduce the risks to the contracted parties. That could lead us to decide, well, let's have the decision-making or the determination part of three.

So there are some questions that need answer before we can actually say, okay, this is where we are going to put the decision making. And then the decision making, so where to put it is one thing, and then if for example we decide to put it on level three, then who would be making that decision? Would it be ICANN or another party? And accreditation also, it could be a totally independent party entity, or it could be ICANN. Authentication as well. it could be a totally independent authentication entity – and I personally think that that would work as well.

So thank you for putting forward this model, and let's think, what are the questions that need to be answered for us to determine what goes where? Thank you.

JANIS KARKLINS: Thank you, Hadia. Greg followed by Brian.

HADIA ELMINIAWI: Janis, I just wanted to say something that I forgot. With regard to Thomas' quick summary over there about what he thinks could work, I just had a comment with regard to the automation part where you said that we would have prefabricated cases based upon which data could be disclosed automatically.

I'm not sure that actually this legally would work, and my idea about automation was quite different. So my idea about automation was if you're defining a user group and with a purpose and a set of data, still, the balancing tests need to be made each and every time.

However, if you automate it, it's done by a computer or a processor, and therefore, it won't take as much time as if its not automated. But it still needs to happen. It's not like you have this case and I'm disclosing based on that without the balancing test. You're automating the balancing test itself. Thank you.

JANIS KARKLINS: Okay. Thank you very much. You see the beauty of face-to-face meetings, that everyone can come to the drawing board and do it like Greg will do now. Please, go ahead.

GREG AARON: I'd like to draw the burger two different ways to show some commonalities and make a couple of technical points. Can I add some space here? Is that okay?

So this is one way to draw the burger, where you have the demand up here, registries and registrars here, and then there's this one central spot, and this might be a system run by ICANN or outsourced by ICANN. This is the model that the Technical Study Group wrote their paper about.

They figured out a technical way to make this work. So that’s something we can keep in mind, that we do have an implementation that’s possible here using RDAP and other things.

And we’ll figure out how people become these parties, how they're accredited and so forth. That’s a conversation we’ll have. But in the end, you have people making requests, they come to a central point. That central point figures out where to send the query, query comes back to that central point, then back to the requestor.

Another way to draw the model is – and I want to make sure I’ve got this right myself – you have requestors and suppliers, but there are multiple gateways. So what does that mean? Does that mean we have several of these in the middle? Okay.

There's also another model which is you et credentials from a central point which says these parties are okay, they can make queries, and then these parties end up talking to each other, but they know they can talk to each other because they're in the system. We don’t have a technical model figured out for this one.

As far as liability, of course, we want these parties to understand what the responsibilities are for dealing with the data. They need to handle it properly, they need to be making legitimate requests and so forth.

Now, in any model down here, these parties are also deciding whether to provide the data or not. if a query comes to them, they could say no, for example, if they feel a 6.1(f) balancing test has not been met. So these parties are evidently able to say no, and they are handling the liability by not fulfilling the query. Thanks.

JANIS KARKLINS: But in this model here, if this central entity says “Yes, the query is legitimate, please disclose data,” in the Technical Study Group model, can data suppliers still say no?

GREG AARON: It could work either way, but the idea was this is a mechanism for saying who’s accredited and shuttling information back and forth. This party might not be saying the request is legitimate. That’s something we would have to discuss. So this is a neutral party that doesn’t make decisions, they just bring information and accredit – not accredit but authenticate.

JANIS KARKLINS: Thank you, Greg. Brian is next followed by Thomas and then Allan.

BRIAN KING: Thank you, Janis. I think for the question that we’re supposed to be answering here, we support using the hamburger framework for our discussions. I feel a bit disorganized right now and I think everybody has great ideas, but we’re not focused on ... We’re not

... Let's do this. Let's pick up a sesame seed and talk about it [inaudible].

JANIS KARKLINS: We're coming there, because I have not heard anybody saying that the model as such is not acceptable. There are variations, deviations, but in principle, that is where we're heading. Of course, devil is in the details, and we need to ask those details to CEO. And I think that this conversation again helps us to think about those questions and details. Thomas, please.

THOMAS RICKERT: Yeah. Thanks very much. Quick response to Hadia. Hadia, you mentioned that you still think that there should be manual intervention for every type of request. At least that's the way that I understood it. On that point in general, I think if we had a chance to get approval for a code of conduct through an authority overnight, I guess we would try to get that, because that's the only way that was seen by the GDPR to get [decent certainty.]

What you would do in such code of conduct is you would write up criteria based on [whether] you do processing of personal data. So I think if you take that as a model that we anticipate with our paper, the idea, at least that's the way I saw it when embarking on this journey, is that we would write up criteria, and if you follow those criteria, then you're in the clear. And that would mean that you would have prefabricated balancing tests for certain scenarios. This is why I think the use cases are a good way to [designing] that.

Automated processing is taking place in the banking industry and the insurance industry all the time, so if we want to benefit from that, we need to come up with the criteria and properly write them up, and only in those scenarios where that fails, we need to have manual intervention. I guess that would ultimately help all parties be shielded from liability. They just need to make sure that they play by the rules that we established, right?

But still, we need to make sure that these rules are right. So shifting the responsibility elsewhere is a nice idea, but if we come up with the criteria based on which, manual or automated decision-making is taking place, we can't move the decision making and we can't move the liability elsewhere. Therefore, I think we need to make sure that we do this as homework. Nonetheless, those who benefit form such systems need to be responsible for their part and indemnify the ICANN ecosystem if they're being accused of wrongdoing.

Also, I think they need to financially contribute in order to cover this, because let’s face it, if we have a policy that allows for the disclosure of data if certain criteria are being met, regardless whether it’s automatic or semi-automatic, if somebody objects to that and if we are being determine by a court that this was wrong, we all have an issue jointly that we need to protect ourselves against.

Therefore, I think that an insurance fund, a security fund is something that we should really bake into our system to cover everybody.

JANIS KARKLINS: So yeah, we'll get there, but the reality is that we're potentially talking about huge amounts of money, if for instance Google now is also a registry, right? So the turnover of Google is how many billions, and 4% of those billions, which insurance will insure that? That's the question.

So Allan.

ALLAN WOODS: Thank you. I'm not going to belabor the point, because I think Thomas has just [said it,] but one thing you said, Janis, where you said that the middle part that whoever makes the decision, the liability rests with them, I fundamentally would unfortunately disagree with that. It's the controller who will always have the liability, and that goes back into what Thomas is saying in his one where you've got that circle and then that circle. The liability is always going out and stretching out, but the liability will always come back to that original controller.

So if somebody is making that disclosing decision on behalf of ICANN, then it is ICANN's liability that is then also shared, but not shared as in 50/50, as in 100/100. It's joint and several. So I just want to be clear that what we seem to be slipping into is the difference between liability and indemnity. What we're creating here is a system of indemnity, not a system of liability sharing, and that is very different for us all.

So I think we need to be very careful with that when we're talking about the way we're creating parties is that, yes, we will be able to put indemnity in there, but not liability difference. We can't [deal with] liability. That's up to the DPAs or the authorities who will ultimately fine us for the wrong decision. So I just wanted to be clear on that one. Thank you.

JANIS KARKLINS: Thank you for raising this, and then maybe that would be on question for the CEO, how Göran sees the division of liabilities in the system, in whatever system we're working out. So that would be a good question.

I have Chris and then Milton. Milton was first, sorry.

MILTON MUELLER: Yeah, I just wanted to emphasize what Brian said. My understanding is that you presented this diagram as sort of the basic framework. We're not really committing ourselves to any policy decisions by accepting it, it's just a framework for discussion.

And it seems like what's happening now is we're getting into the discussion as part of the discussion of the hamburger rather than confirming the overall approach and then getting into those discussions later. So I would like to stop discussing the hamburger and start discussing the substantive issues as soon as possible. Thank you.

JANIS KARKLINS: Thank you. Chris?

CHRIS DISSPAIN: Thanks. I'm more than happy to accept [inaudible] Alan just said, but I understood that liability or being a controller is to do with why you have the data. So if a registrar gets the data to register a domain name, they have that data they need in order to register a domain name is that data and now they're the controller of that.

If they collect the same data or a subset of that data for a different reason as a processor, and pass that on to someone else, that someone else is the controller. That's correct.

Well, no, I get that, but I'm not asking you about that. My understanding is that's how it's supposed to work, that you can collect the data and pass it – so if you take a very simple example – yeah, right – ICANN has a valid purpose for collecting the data. Forget disclosure, just talking about holding it for the moment. ICANN has a valid purpose for holding that data. If you collect that data on ICANN's behalf and pass it to ICANN, and that is a valid purpose, you're not liable as a controller; are you? You are?

ALLAN WOODS: So in that instance, what you're talking about – I'm going to have to take it from there. Let's just say that the registrar is the processor and ICANN is the controller in this instance.

CHRIS DISSPAIN: For this particular purpose, yes.

ALLAN WOODS: Yeah. Under Article 28, you as a processor cannot process that data unless you believe that it is in line with the law. So if you process that data even though you know that it's not in line with the law, you are then liable, and that was one of the changes in GDPR – and being very specific to the GDPR at the moment, that is an important thing.

CHRIS DISSPAIN: Yes, but what does "Even when you know that's not in line with the law" mean? Because that's a meaningless phrase unless you have a finding that something is not in line or in line, in which case that means that the only basis on which you can do something, guaranteed, is that there has been a decision made that says that that thing is okay.

That's a logical thing, isn't it? Because this is not [black letter law,] it's a principle thing, right? Okay. Cool.

JANIS KARKLINS: So yeah, I think that this should be conversation with a coffee mug in hand during the conversation between interested parties, because it is essential to get that understanding right and then coming back to inform the rest of the group on the outcome of that conversation. And it also actually would be good if Dan could participate in that conversation as well when it will happen offline. Mark, are you ...

MARK SVANCAREK: I want to support what Chris said. It's in line with what Microsoft believes. However, I want to recognize Allan's concern that this really hasn't been confirmed in any real way. So we believe that's the intent and we believe that's going to be the outcome, but there's no assurance at this time. So I recognize your concern about that.

JANIS KARKLINS: Okay. Volker?

VOLKER GREIMANN: Yes. Just to qualify this, what Alan said, when you said that what you believe to be not in compliance with the law, it doesn't really matter what you believe. It matters what the fining authority believes is in compliance with the law.

So if you are being fined for a violation that you thought or an action that you thought was actually compliant, you're still being fined. That can be that finding [inaudible]. So even though you feel that you are complying with the law by implementing whatever we're deciding upon, if the DPA doesn't agree with that, they can pick and choose whomever they want in that chain of people that process the data or control that data to place the fine upon.

JANIS KARKLINS: Dan, you're the last one, then we will break.

DAN HALLORAN: Thank you, Janis. I just want to chime in, for ICANN Org, of course, we're happy to proceed with the hamburger model. I think it's important to note that today, we have the two buns. You have the demand and you have the contracted parties with the data, and there's no beef in the middle. So we're trying to build the beef.

VOLKER GREIMANN: Vegan meat replacement.

DAN HALLORAN: That's called an impossible burger. So we have that today and we're happy with the model. I was also very interested in Allan and Chris' exchange and I'm happy to go into that with [coffee,] but also – just that's a preview of the conversation we'll have with Strawberry. That is the Strawberry question, is, if you take that decision-making out of the bottom bun and move it up to the middle hamburger, are the contracted parties still liable for that decision-making? That's what Strawberry's been working on. Thank you.

JANIS KARKLINS: I think now we have some sense that we need to clarify during the meeting with the CEO. I do not intend myself to try to speak on your behalf except I would ask those two questions that I sent in writing on our behalf as a formulation, and I will ask CEO open question, meaning how he sees the place of ICANN in the system that we're building. And after his response, I will open the floor for everyone to ask clarifying questions after his explanation.

And we will revisit this general conversation about the model, architecture of the model as a result of conversation with him and the Strawberry team. And the Strawberry team as well, I would ask those two questions that were addressed to Strawberry team, and after response, we'll invite you to ask any clarifying questions that you may wish to give.

I think that this is an important, crucial moment in our work to try to identify and understand all the limitations that ICANN may have in developing this model, because if we – ideally, we would need to get out common understanding what is possible, what is not. And if that would be the outcome, then we could work towards a possible model. That would be my conclusion after this conversation.

So with this, I would suggest we take now a 15-minute break.

GINA BARTLETT: [inaudible].

JANIS KARKLINS: Yeah, the questions are on the screen, and once we come back, then we'll start talking about building blocks, taking first building block accreditation and associated question on user groups. And I encourage during the coffee break interested members join Alan and Chris in their conversation about – no, you need to work, Chris. You asked for it, you got it. So 15-minute break.

GINA BARTLETT: [inaudible] right after lunch, and then we have time allocated to come back to that. So what we'd like to do in the meantime is go ahead and continue working with the building blocks and start with building block F on accreditation.

What we thought we'd do is Marika will frame up some of the comments that were received and then both Milton and Alex have provided a proposal for consideration, so we thought we would go to Milton and then Alex to walk us through those proposals, and then we'll open it up for discussion from there. Marika?

MARIKA KONINGS: Yeah. Thanks, Gina. We'll just put up on the screen the cutout from the latest version of the zero draft, the text that's currently in there in relation to accreditation as well as some of the high-level input we received from everyone and then to frame that up for subsequent discussion.

So the language that staff included there I think was actually largely based on a proposal I think that Alan Woods circulated to the list at some point, so we kind of took what he put in there and framed it up in a way referring to user groups being responsible for self-organization and developing a proposed accreditation mechanism that will be shared with the European data protection board for review.

I think we already flagged in the report that it wasn't actually clear to us how that would actually work in practice and what will be required, and it had as well a number of principles that would need to be followed as well as requirements for those wanting to be accredited to follow.

And also the notion that of course failure to abide by those rules would affect accreditation, including the possibility of revocation. I think there we also flagged a question, what does it actually mean when your accreditation is revoked?

This is basically what we devised from the input that was received from the different groups on the zero draft. I think an overarching question that was flagged was, is accreditation necessary? I think there was also a suggestion to consider equating accreditation certification under Article 42 and 43 of the GDPR [inaudible] flag the questions, are there any other forms that could provide anything other than verification of identity? Where that may fit in the chain. I think someone else has suggested that this might be a list of enforcement considerations and there might be more needed.

Also this question on who would be responsible for revocation? Would that be the SSAD or accreditation body? But if it would be the accreditation body, who would be kind of checking the accreditation body that they would be following the rules? And I think there was also a suggestion that bullet four would need to be clarified, what is actually required, and I think that related to the maintaining of registrar of all requests, also including the respective rights holders' name.

So that was something that we at least derived from the input received, but it was really just a starting point, and I think that has already been added to by the different documents that were submitted by Milton as well as Alex.

GINA BARTLETT: Should we tackle the “is accreditation necessary,” or should we go to the proposal first, Marika? Proposal? Okay. So Milton, do you want to walk us through your proposal first and then we’ll come to you, Alex?

MILTON MUELLER: Wanna put it up on the screen, or can people have it from the mailing list?

GINA BARTLETT: Terri will put it up on the screen, but if you want to go ahead and start, I think everyone does have it in the mailing list. Thanks.

MILTON MUELLER: Okay. I wrote this memo mainly because it appeared to me that people were attaching the label “accreditation” to very different things, and I wanted to tease out the differences and clarify them.

When I heard the word “accreditation,” particularly when it was talked about as a means of enforcing adherence to proper use of the system, I had in mind – and many of us in our group had in mind – something like proposed purpose one, which is accreditation is an agreement that provides parties requesting disclosure with ongoing permission to use the SSAD while binding them to a code of conduct governing their access to and use of the disclosed data. It also provides an enforcement mechanism so that you can withdraw or limit that accreditation in cases of abuse of the data.

Now, we heard another purpose, and it’s closely linked to the concept of user groups, so that is the idea that there would be some kind of external organizations or entities that would represent or have legitimacy among user groups. We've heard WIPO mentioned by Thomas as somebody who could accredit trademark owners for example. We've heard about the lack of a single obvious entity to accredit cybersecurity researchers.

But anyway, this second approach to accreditation is tied to user groups, and it’s sort of a way of certifying if parties are legitimate members of a recognized user group.

So I mainly want to make the point of how different the implications of these things are. We may push towards eliminating one or both of them. We may try to hybridize them. I don't know what we’re going to do, but I just want to be clear about these differences.

So in terms of who performs it, if you're thinking along the liens of the purpose one, there has to be a close link between whoever is administering and operating the SSAD and the accreditation or the ...

So that could be ICANN or it could be whoever is operating the SSAD, and of course, if it’s ICANN, it could be outsourced to somebody functionally, but still, ICANN would be responsible for it.

For purpose two, that would be, again, a potentially unlimited number of external groups. It would depend on the number of user groups. So I think in terms of the implications, one of the concerns we have with purpose two is, do you need to accredit accreditors? Are you adding a layer of activity here? Would external accreditors be exclusive for each user group category? How mutually exclusive are these groups? Can you really slice the world up into a set of mutually exclusive groups that can be accredited? And what if you had competing or multiple parties proposing to accredit groups? Would you get into a race to the bottom? Could there be a link between enforcement and these external groups?

I don't see how that works since the main reason for accreditation is to facilitate access to data. How interested would these external groups be in enforcing accreditation by limiting access to data? And wouldn’t there still be a need to have a contract with the SSAD imposing a code of conduct even if you had the other form of accreditation?

So that’s just by way of facilitating discussion. Hopefully a clarified discussion about what we mean when we talk about accreditation.

GINA BARTLETT: Any questions for Milton? Because what I would propose is we go to Alex and then open up the conversation on who and how this proceeds. Questions for Milton? Oh, Hadia and Alan. Alan was first. Excuse me.

ALAN GREENBERG: I've put this in the e-mail, but I'm a little bit confused. What you have as purpose two doesn't sound like a purpose to me. It sounds like one of the methodologies, one of the processes we may use to effect number one, but I don't see that as a purpose, and I don't recall anyone talking about that explicitly as a purpose.

MILTON MUELLER: I would answer that by saying the purpose two is that you are essentially recognizing or authenticating somebody as a member of a group. That's what many people mean by authentication. And the process by which you do that is completely undetermined so far. But again, if you believe in purpose one as the main point of accreditation, then you may not even think you need purpose two, you don't need that process at all.

ALAN GREENBERG: To be clear, I think we need the process, but I don't see it as a purpose for ICANN or us. I think it's one of the mechanisms that we're going to end up probably using in some cases.

GINA BARTLETT: Milton, did you mean that as a purpose in the capital P purpose, or more of a definition?

MILTON MUELLER: Absolutely. I think both of these purposes that I've defined imply processes to implement them. But it's definitely a different approach to accreditation, a different objective, if you will, than the other one.

GINA BARTLETT: Thanks. Hadia, and then I have Mark.

HADIA ELMINIAWI: I would go back to the definition that Milton put. When he says it’s an agreement that provides parties [inaudible], no, it’s not an agreement –

GINA BARTLETT: Hadia, can you get closer to the mic?

HADIA ELMINIAWI: Yeah, sure. So no, it’s not an agreement that provides parties requesting disclosure. It’s actually a statement from an accreditation body declaring that specific requirements are met, and based on that, certain entities have permission to use the standardized system for access and disclosure.

And then also, you linked the accreditation entity with the access, and actually, no, accreditation entities only accredit parties that meet certain requirements to use the system. But whether actually they will have the data based on that or not, that’s another issue. So it doesn’t give them access, it just gives them permission to use the system or make their request through the system.

GINA BARTLETT: Thanks, Hadia. Mark S.

MARK SVANCAREK: Mark SV.

MILTON MUELLER: May I respond to Hadia first? I think she's kind of misread the document. In both cases, accreditation does not guarantee disclosure. That’s clear form what I said in both cases.

When she says that purpose two, accreditation is a way – I think one of the key differences between these two is that what I'm defining as purpose one, there's one accrediting entity that’s closely associated with the SSAD operation. In hers, purpose two, there's potentially multiple parties and they're not directly connected to operation of the SSAD, they are simply external parties.

So the distinction does exist, and it’s very important.

GINA BARTLETT: Thank you for the clarification. Go ahead, Mark S.

MARK SVANCAREK: Mark SV. First comment. I think we’re already diving in too deep, so we’re already violating our process here because we haven't even heard from Alex yet. My comment though was if you could scroll up to the top of the page, so when I read Milton’s memo where he says purposes, I was actually thinking that they were definitions, so people are using the term to mean different things and he says some people are using it in this way.

So I don't see these as purposes so much as "Here's one definition of accreditation that people are using and here's another definition of accreditation that people are using." And I'll refrain from discussing the substance of those until we're later in this discussion. Thanks.

GINA BARTLETT: Thanks Mark SV. Excuse me. So thank you for those clarifying questions and some substantive contributions. Let's go to Alex Deacon. Alex, if you could walk us through your model, we'll do that, and then we'll start opening up and tackling some of the issues.

ALEX DEACON: Thanks. While it comes up on the screen, let me just tee this up. So I've been listening to the conversations we've had on the phone and here, and then also reading through the comments on the zero draft. I think we need to pop up at least one level in our discussion. What I've tried to do is put together a framework to assist.

When reading principle one in the zero draft, it mentions things like predictable and transparent and accountable. So this accreditation framework that I've put together kind of keeps those in mind.

So I'm going to try to not deep dive and keep things pretty high level here in terms of the details behind each of these boxes as we know there's lots going on.

So I think in order to adhere to this principle number one, transparency, predictability and accountability, we need to do two things. We need to set a baseline policy for accreditation and accreditation bodies, and we need a process that kind of onboards them or manages them through their life cycle. This also means if something goes wrong, they could be offboarded.

If you look at the diagram here, it’s a little bit complex. I tried to make this linear to simplify things, but there's a lot of interrelation, so bear with me as I go through this real quick.

To answer some of Milton’s questions, I think we do need to accredit the accreditors, and this kind of sets out how I think one could do that. So let’s dive in.

I think on the left, in the blue, we have basically – this is where we’re sitting. We need, as I mentioned earlier, an accreditation body baseline requirement policy. This is the policy that’s at a minimum an approved accreditation body within the system needs to meet the following set of policies and requirements.

This makes sure that there is this predictability in the system and accountability and transparency in the system. Everyone will know what the accreditation body is doing at a minimum. Clearly, based on the user group that they represent, there may be additional requirements placed on top. That’s fine as long as they adhere to the baseline policy, then all is good.

Then if you look at the bottom left, there's the trusted accreditation body program policy. This essentially defines, at a high level, what is required for an accreditation body to be trusted in the system. And I won't go into the details there, but this is an important part of how, again, accreditation bodies are approved and then eventually removed if necessary.

At the top, you'll see that the accreditation body baseline policy will be used by the accreditation body to create what I've called an accreditation body practice statement. This is essentially the accreditation body saying "Here's how I adhere to the baseline policy requirements" and essentially how the accreditation body is going to implement that policy in reality.

I think this concept of auditing is important. In the middle there is an accreditation body auditor. Could be a third party or ICANN, or again, I don't want to dive into exactly what that is, but that role I think is important.

They will audit and perform an audit on the accreditation body to make sure that their practices are in line with the policy, and then when that audit is completed, they will provide that to – at the bottom middle there – the accreditation body approval and onboarding organization.

So this is essentially the implementation of this policy [inaudible]. And they will use the set of checkboxes in the policy set by the trusted accreditation body program to determine which of these accreditation bodies can actually be trusted within the system.

And this is, again, to answer I think a question or to address an issue that Milton raised, I think there is a tight binding between the organization that determines who's in and who's out and the SSAD, and again, to ensure predictability, transparency and accountability.

Another way you could sliced and dice this diagram is on the left. The left column, if you will, is the policy. The middle column is kind of the implementation of the policy, and then the right column is the [operalization] of the policy.

So once the accreditation party has been approved, then requestors – those are those three people in the middle – will enroll, if you will, to one of the bodies based on what data they want to access in the system. The accreditation body will follow the procedures and guidelines that they've laid out in both of those documents, plus any additional requirements that they may require, and once that individual has been verified and validated, they will be issued a credential. If they don't meet the requirements, then the credential won't be issued to them.

Assuming the credential has been issued, the users will then use this credential which identifies them to the system when making a request to the SSAD, and because the accreditation body has been approved and trusted within the system, that credential can be validated as legitimate, and the identity verified by the SSAD system itself.

And then what happens in the middle of this hamburger occurs, so we won't get into those details.

In terms of revocation, I think this came up a few times. I think there's two opportunities here for revocation. One is if an individual user who has previously applied to an accreditation body is found to be doing bad things, then the accreditation body can revoke that single credential and thus blocking access to the SSAD:

If it turns out after audits that the accreditation body has just gone rogue, then the full accreditation body can be revoked, if you will, and then any individual who's been accredited and credentialed by that specific accreditation body will be blocked access to the SSAD.

So this is my view. To be honest, I did not vet this with the IPC. I shared it with them. In my mind, it's logical. It is based on similar policies that exist in the security space, specifically how browsers trust roots of certificate authorities, and I guess I'll leave it there. Happy to answer questions.

GINA BARTLETT: Okay, so let's ask clarifying questions of Alex, and then I think we need to get into the requirements from the policy standpoint and the who. And Alex has just articulated a number of whos, I think. So I have Hadia, James, and Janis.

HADIA ELMINIAWI: My question is with regard to the credentialing part. I don't understand quite how did they get – so those user groups were accredited by this accreditation body, and then the accreditation body also gives them the credentials. So authorization, so it’s an accreditation and authorization both?

ALEX DEACON: Yeah, so again, I've tried to keep things high-level here without getting into those details. It could be both.

HADIA ELMINIAWI: It’s just because you’ve put the credential use going directly into the [SSAD,] and that’s why my question, that’s why I did ask.

ALEX DEACON: Yeah. Again, I'm trying not to get into the details. It’s going to be a credential that authenticates the individual so you can know who the identity of that individual is and authorizes their access to the system.

HADIA ELMINIAWI: For the time being, I would actually remove this arrow going into the [SSAD] since we don’t have any block that says that we did any kind of authorization or authentication. But yeah, that’s just me.

ALEX DEACON: Okay.

HADIA ELMINIAWI: I won't get into the other details.

GINA BARTLETT: Thanks. James, Janis, and then Milton.

JAMES BLADEL: Thank you. And I'll just be brief, and obviously, we haven't had a chance or an opportunity to fully kick the tires on this particular model, but immediate reaction is this is a very robust, comprehensive and detailed, but I think it addresses a lot of questions that we had about how this would work. It also I think introduces a lot more functionality in terms of accountability and transparency that maybe we hadn’t considered. When I say we, I mean we as a group but also we as registrars.

So I think I just want to say thanks to Alex, tentative and cautious enthusiasm for this model and want to take it out and drive it around a little bit and kind of see how it operates, but I think that it is a very useful model. So thank you.

GINA BARTLETT: Great. Janis?

JANIS KARKLINS: Thank you, Alex. I have actually two questions. One is, in your mind, how many accreditation bodies we would have in the system? And the second question is, some of those organizations that would potentially make accreditation were already named, WIPO and Interpol or Europol. Would they also go through the accreditation of accreditation bodies? Because they are kind of authoritative entities, intergovernmental organizations in reality that are working in specific areas. They are already recognized as authorities in the space. Would they also need to go through the accreditation process to become accreditation agents?

ALEX DEACON. To answer your last question first, I think the answer is yes, they would have to go through this accreditation process to make sure they're adhering to the baseline policy requirements that we will need to set.

On your first question as to how many accreditation bodies could there be, again, this framework doesn't really care. There could be one or 20. It will work no matter what model we eventually come to. I think obviously if there's one, then things become a lot simpler, but this framework still applies.

GINA BARTLETT: Milton?

MILTON MUELLER: Yes. I sort of indicated the general [inaudible] of my question in the group chat, but let me just follow up with that. The good thing here is that you have agreed in effect with my analysis that this kind of accreditation, purpose two accreditation is an additional layer, it's not a substitute for the other kind of accreditation. So we still have to have ICANN accrediting accreditors, we still have to have some way of withdrawing and granting accreditation rights to these third-party organizations.

So we have an incredibly complicated bureaucracy, and you've just admitted that it's open-ended. There's no potential specific limit on the number of parties that would be seeking approval as an accreditation.

So I just don't understand what this accomplishes that isn't already accomplished by having a single accreditation contract that anybody can sign. I see it oddly as limiting and distancing ordinary people from using the SSAD by introducing this complex system of intermediation.

I see the categories of user groups that would be invoked by this as being overlapping and not clearly defined, and I guess, just what does this accomplish? Why do we need this?

ALEX DEACON: Yeah, thanks, Milton. When I put this together. my focus was on how do we create or how can we create a framework that handles the likes of WIPO and others who may be accrediting groups of folks. This does not – and just to clarify, this does not disallow individual users from accessing the system. They just wouldn't be accredited by an accreditation body. They would be authenticated and authorized via some other TBD means.

It seems to me that if we want to enable a situation where there are N – where N is undefined – accreditation bodies aligned with user groups, then this would be the way to accomplish it.

GINA BARTLETT: I have a really long queue. What I was going to propose is that in a few minutes, I'll go through the queue, but that we break into caucuses and you talk about the idea around Milton's proposal on the purpose and definition, the requirement for an accreditation body or bodies, and then who might serve as the auditor and the revocation body.

So to talk in your caucus and then come back together and continue that conversation. So that may affect whether or not you want to still have your card up, but I have Allan next, Ashley, Mark SV, Alan, and Greg. Is this another Alan, the Alan G? Go ahead, Allan Woods. Alan G. Sorry.

ALAN GREENBERG: The Alans have agreed that we think I was the first one. This model pretty well fits what I had imagined. However, to answer Milton's question of why should we do this, which is admittedly a complex process which we're going to have to build and it isn't going to happen overnight, I think the answer is because we're subdividing the work to groups that actually know how to do it instead of trying to invent one amorphous group that suddenly can recognize a lawyer who has credentials in certain areas versus an intellectual property expert versus a security expert versus whatever.

So what Milton is describing, surely we could do it, but I think it's going to be almost impossible to build because although it's a simpler structure, it's going to be really difficult to do whereas this, I think although it's more complex and interconnected, we can assign responsibilities to groups who actually know how to do it, and Interpol and WIPO are examples.

Again, I agree with Alex, you still have to accredit them because you need some paperwork, but it might be a very much simpler accreditation process to accredit them than to accredit the group who recognizes security people, which is an undefined quantity.

So although I'm overwhelmed by how much work we're going to have to do to build this, I don't see a practical way of doing it in a single amorphous model. Thank you.

ASHLEY HEINEMAN: Thanks. Yeah. I'm going to do my best not to get too weedy on this, but I think it's a good baseline conversation. So in terms of accrediting bodies, I think we just need to be clear – and I'm not saying what I'm thinking is the right way, but just my view – is that the purpose of the unified access model is to basically come up with something at least as I understand, it's going to make it easier for those who request this information on a regular basis with a legitimate interest in general that we recognize.

So we're not trying to cover accreditation for every schmo out there that wants to have access. And that's not to say that their needs aren't important, it's just that that's not what this access model is for. They will always have the right and the ability to go directly to the registrar. Okay, so it sounds like we're on the same page.

Now when it comes to how many accrediting bodies, I would say that we shouldn't take one off the table necessarily. I agree with everything that Alan Greenberg just said in the sense that we should build off of those who have the expertise, but there might be creative ways in which they could be responsible for developing the requirements but not necessarily responsible for doing the accreditation.

So just not to take it completely off the table, but I would also put an outward limit, at least for this initial exercise, try and say no more than three because it's hard enough as it is. Let's not make it any more difficult at this point in time. So I'll shut up. Thanks.

GINA BARTLETT: Okay. I've got Alan Woods, Mark SV, and Greg. And then I'm going to check in and go to caucus if possible.

ALLAN WOODS: Thank you. So I appreciate both the way that we're thinking about this at the moment, but I still want to link this to a very more fundamental question, and that is, me, assuming I'm the person making the decision, what will accreditation do for me? What will it confirm? What will I be able to add to my decision-making process from this creation of an accreditation?

So at the moment, all it goes to is identity. That's all, and that is one element of – yeah, it's helpful for me because then I can confirm this is a person who's making that request, but I can also do that through very simple means and not through a convoluted practice of accreditation.

What we should be aiming for is we're trying to take the burden away from the person making the disclosure that they can rely upon this accreditation for things like [that they] are going to do with the data that they're going to suggest, that they are going to be in line with the GDPR as being one data protection element.

That one for me is the big one, because if we can assume that a person is compliant with legislation, then that takes an awful lot of the emphasis on us. But unfortunately, there's only one body out there who can actually do that accreditation, and that is – well, there's none at the moment, but – actually, there's one, sorry, and that is who has been certified by the European Data Protection Board or the Data Protection Authority. They're the only people in the world who can certify a body to be an accreditation body, and that's what Article 42 and Article 43 references.

So the goal for us to spend all this money and time and effort and trying to figure out what accreditation is, it must be linked to what is the benefit for us making that decision. And I'm sorry, at the moment, if it's just identity, we may as well move on because that's not good enough to spend all this money and time and effort, because it's not going to add anything to us.

But if we go that extra step and get that huge level of formality, well, then it is a worthy enterprise. But until we figure out why we need it -and that would be the first question I put on the team, is, why? It would be helpful, but at the moment, I don't see [spending a day on talking on this number.] I know we're not, but ...

GINA BARTLETT: Okay, I see you, Alex, but is it okay? Okay, [you have a problem with him responding?] So go ahead, Alex, respond brief. If you can be as concise as possible.

ALEX DEACON: I agree. So I think this needs to be much more than just identity, and thinking about what Thomas drew on the board earlier, I think there's alignment there. I think you could think about the policies across the top accreditation baseline practices statement. I think that may be some form or start of a code of conduct. I think you could build this in such a way where you are doing this in a GDPR-complaint way and we end up with a code of conduct and a process around to enforce it. So yeah, if it’s just identity, I agree. There's not a lot of use here. We need more than that.

GINA BARTLETT: Thanks. Mark SV.

MARK SVANCAREK: Alex, I love this. I do think that it still falls into the problem that Milton calls out, which is that the word “accreditation” was not actually defined here, so this is kind of a mix of there's a credential body or somebody giving out “This is who your identity is,” there's a code of conduct monitoring body here. I think all these things are sort of mixed up together, and which I think would make Alan Woods’ goal more clear, like how do we turn this – which I think is pretty robust and complete – into what he needs, which is the formalized process which has been vetted and approved by a DPA?

GINA BARTLETT: Volker, and then we’re going to caucus.

VOLKER GREIMANN: Okay, just a brief point. I fully agree that this needs to be more than identity. I think this can be achieved by marrying this to the purpose one that Milton proposed or outlined in this proposal.

There's a certain dependability and trust and process already baked into that that contracted parties would be able to rely on when we receive a request that is in some form backed by this accreditation body.

One thing that is addressed here and that I would just like to point out as a potential problem is that we should be aware that any accreditation body might be seen to be in the camp of the entities that it accredits, for example, if you have an accreditation body that is responsible for accrediting security practitioners, it probably is a community of security practitioners that built that body up and accredits its members. We need to be sure that there's certain safeguards against that kind of capture or that kind of self-interest being baked into the accreditation body that we would have to defend against.

GINA BARTLETT: Okay. I have Hadia begging me, and I just see Brian, so super briefly, please.

HADIA ELMINIAWI: Just to Allan's point, how I actually envision accreditation is far beyond just identity. And Alex did mention the code of conduct and all that. But also, you accredit a group of people to access the system for a certain purpose and for the disclosure of certain records.

So it's people, purpose, and pieces of data. And that's where the benefit lies from my perspective. Thank you.

GINA BARTLETT: Okay, so let me see if I can frame what I would like you to talk about in your caucus kind of based on what we're hearing. I think Ashley's point that we're not talking every Joe Schmo and Jill Schmo, it's the purpose of providing a universal accreditation for legitimate interest. It's not just everyone. You have a little bit narrow audience.

UNIDENTIFIED MALE: [inaudible].

GINA BARTLETT: Oh, you don't accept that? Okay.

UNIDENTIFIED MALE: [inaudible].

UNIDENTIFIED MALE: Microphone.

GINA BARTLETT: Okay, so the point was that those who have legitimate interest and those who don’t. So there's not agreement that you could identity the accreditation system for those who have – to determine the legitimate interest and have legitimate interest? No. Okay.

Well, I think we could still make some progress potentially, and what we would like you to do – what I was thinking on the caucus idea was to talk about the purpose as Alan Woods defined it. Maybe more than identification, it’s also removing the burden from the entity providing disclosure. And I heard your part around also who certifies who the accreditor is.

The policy, what are the requirements needed, and then the who, with Alex’s proposal, he identified a number of those whos, right? Who is the accrediting body, who is the auditor, and who does the revocation.

And what I was going to propose is that we think about this in terms of Milton’s purpose one around the accreditation to provide access to the SSAD. So not the [sort of a niche] like the user groups, but rather focus on the accreditation.

So why don’t we take 10 minutes in your group and then come back out? Is this clear enough? And talk through some of these issues, and let’s see if we can advance this building block another step beyond where we are right now.

Can everybody grab a seat and can we get started? Welcome, Stephanie. That corner, do you need a few more minutes, or are you okay? You're okay?

Okay, so thoughts about the purpose. Maybe we start with the purpose and hear a little discussion on that, and then we can go to the policy requirements and then the who, but the purpose around identification, removing the burden from the entity providing disclosure, and what else is needed to make it worth the while of developing this? Thoughts about the purposes?

ALAN GREENBERG: I think the main thing that’s missing from purpose is it provides a level of trust and confidence to the contracted parties that the person they're dealing with is someone they can ... If they had to do the balancing case themselves, they would say yes. It’s a level of trust based on the overall process that they know has gone before allowing someone to get appropriate credentials or a token to pass on to them [inaudible].

GINA BARTLETT: I'm sorry, I didn't realize that we had lost our Noncommercial Stakeholder Group. I thought that people were there. I'm so sorry. Okay, we’re just going to pause a second. Sorry, Alan, we might ask you to repeat your comment.

Okay, so we’re going to pick up again where we just started. Stephanie, welcome. Would you like to introduce yourself?

STEPHANIE PERRIN. Yes, I’d be delighted. Stephanie Perrin, I'm the Noncommercial Stakeholder Group.

GINA BARTLETT: Welcome. So what we were going to tackle was picking up from before the caucus, thinking about the accreditation and starting with the purposes of not only identification and removing burden from the entity that's disclosing, but what else would be necessary as a purpose in this context in order to make it wort the while.

Alan G, Allan W, and then Brian. And then Milton. Thank you.

ALAN GREENBERG: Thank you very much. The item that's missing from purpose that is absolutely crucial is it provides a level of trust. Specifically, it gives to the body releasing the information a belief that this unknown requestor, if they had to do the balancing act themselves, would decide to release the information.

So it's giving them a level of trust and confidence that the entity they're dealing with is someone who has a valid reason and they won't get into trouble by releasing the information, effectively. Thank you.

ALLAN WOODS: Thank you. So I think, again, looking at the breakdown [if there's the] third parties or not. Let's look at third party for the moment. I think listening to a few of the conversations as well, there's a suggestion – just bear with me for a second – that just because somebody says that we should be able to trust them does not mean that we can accept that trust.

So in order for us to accept a third party accreditation, we need to identify – and it probably would fall to ICANN in this concept – that we would need to actually audit an accreditor and probably a sample of accreditees in order to assure or to see whether or not their statements are correct.

So an accreditation body in order to make it effective – and again, going back over what I said very briefly, it must be more than just identity. It must be more than just trademarks, to be perfectly honest, because a trademark is a publicly available thing. You can check that up for yourself. That would be what I would do. You're having nothing, you're just creating a large process to confirm something that’s publicly believable.

So what we need to do is ensure that if somebody is coming to us, that the accreditation body is doing things like they're testing whether or not a purpose is limited to the purpose which they state. They're testing that data will be held for only as is necessary and will not be used for any other purpose. Things like this are the things that we need to be able to rely upon as a disclosing body.

And if they're coming to us saying, “Well, no, you need to trust us,” we can't unless we can demonstrably show that we have gone through the process of testing that trust. And that is a huge additional burden on what we’re trying to do here.

So the suggestion from me is that – and I'm sure Milton will have issue with this in a way – they should come to us. We shouldn’t be saying to them “This is the accreditation, this is the process by which you get accredited.” They should come to us and sell us the accreditation saying, “This is how you can test us, this is how you can test that what we're saying is true, that we are in line with the laws," not just the GDPR because I know I have a very GDPR-centric head, but there are other laws that need to be taken into account, and we need to trust them as well.

So they need to present to us their system of accreditation and ICANN would need to then test that system of accreditation. Whoever the disclosing body is needs to test that system of accreditation,

Why I keep going back to the example of the Article 42 and 43 is that if they are certified by something that has been signed off by a DPA- or again looking at the Article 40 that Alex was just talking about, which is the code of conduct, we can rely upon that trust without having to actually test it ourselves because that trust is sourced from the legislature, basically. It's from the data protection authorities themselves. Therefore, we can say "Yes, they are accredited, they are accredited by a certified body, and therefore we can rely upon that." We don't need to test that, we don't need our audit, we don't need our assessment.

So that's the level at which I'm pitching it. it is a very high level of trust required, and it's easier for us and for everybody involved if that high level of trust is through a DPA or the equivalent in another legislature.

It is very high-level so that we can trust it. That's where I'm coming from.

GINA BARTLETT: Thank you. Brian?

BRIAN KING: Thank you, Gina. James, to your question about the purpose here, there are a couple that we don't have on the board that I wanted to add. One is that the party requesting to ultimately become accredited should have an agreement in their accreditation application in which they agree to process the data in compliance with GDPR and all data protection laws, it helps Allan or whoever's going to make the determination to make that easy.

So that's part of removing the burden. It might be kind of a sub-checkmark on the checkmark you have there, but that's something that we think is important.

Another purpose is that this has the potential to spread liability out a bit. If there could be liability for the accrediting party, for the accredited party, for others in the system, so that's potential benefit.

And then also to – I think Volker asked the question about the alignment of interests of the party that's providing the accreditations with their members. one thing that we were thinking about is if the accreditation body is subject to being deaccredited and that results in the deaccreditation of everyone that was accredited by that body, that serves as a check to keep that accreditation body honest and to keep its members from abusing their accreditations, because then the rest of their fellow members will be super mad at them.

So that's the concept that we're thinking, is a nice built-in kind of failsafe there. Thanks.

GINA BARTLETT: Thank you. Milton, Volker, and then Mark SV. And then Stephanie.

MILTON MUELLER: Okay, so we did the caucus about this, and we're pretty much in agreement. If anything, our opposition to what we call purpose two accreditation has strengthened. We believe very strongly that if for some reason you decide to go down this crazy route of certifying certifiers, you cannot link those groups to user groups.

User groups have a specific interest in access to the data and their members have interest in access to the data. If you want some kind of external accreditation body, it has to be something along the lines of what Allan is suggesting, the sort of data protection-related certification. I don't think anything else is going to provide the trust.

We also discussed Alan's argument, and there was some sympathy for Alan Greenberg's argument that these third-party agencies might know more about their user group than ICANN would and would be in a better position to accredit them, but in the end, again, in order to keep them accountable, and because of the conflict of interest between a user group and data protection, ICANN would ultimately have to know enough to be able to know whether these groups were doing a good job at certifying their members or accrediting their members. So you don't really escape the need for ICANN to be on top of this situation.

If you try to put it down into a list as to what can go wrong by allowing somebody to use the SSAD, you come up with a fairly small but really critical list of things, and it’s not clear that the accreditation helps with any of them, frankly.

One is that they could lie about who they are and what their purpose is. In many cases, that might be helped with this external accreditation. You would say, “Okay, I'm confident that they are an intellectual property owner,” but as Allan said, there's other ways to do that.

And there's no guarantee that somebody who is accredited by a user group would not also lie about what their purpose is, and therefore you still have to be able to audit that.

There's a danger that they misuse the data. Again, accreditation doesn’t help with that at all. And you have to determine whether to disclose the data in response to their request, and accreditation as we have admitted as a principle absolutely does not tell you that you are going to disclose in any particular case.

So we’re still with Allan on the question that identity alone is really not worth all of this stuff, and the only kind of accreditation that we would consider would be coming from sort of the Article 42, Article 43 approach that was suggested. Thank you.

GINA BARTLETT: Thanks. I'm going to keep going through the queue, but it would be very helpful if we could hear your thoughts around this question on the table if this Article 42, 43 would be the primary certifying or the legislature, DPAs, or there could be some other way of identifying the accreditors.

ALAN GREENBERG: Point of order. Right now, I thought we're just on purpose and we'll then go to policy and who later.

GINA BARTLETT: We're trying to focus on purpose.

ALAN GREENBERG: Okay, because I'm hearing a lot of discussion about the who right now, the audit [inaudible]

GINA BARTLETT: Right. And I'm hearing a lot on the requirement –

ALAN GREENBERG: Which I've reserved my points on. I thought other people were supposed to also.

GINA BARTLETT: Okay. Thank you for that reminder. So if we could stay focused on the requirements for what would make the system worthwhile, and I'll summarize that in just a sec, and then we'll come to the requirements. And I've been pulling some requirements out of the conversation that I can summarize. Volker.

VOLKER GREIMANN: Yes. I fully agree with what some of my predecessors said, that the purpose should also be that certain enforcement of a code of conduct should be baked into that process.

What the purpose should however not be accreditation process is take away any part of the balancing test, as Alan [Greenberg] suggested earlier, and the balancing test is still very much part of the purpose that is given for every individual request, it has nothing to do with the accreditation of the requestor. That takes .... Certainly [inaudible] consideration in that balancing test that has to be done later, but it is not part of the balancing test itself. That separate test has to be conducted on an individual basis per request.

GINA BARTLETT: So Volker, would you then have the accrediting process primarily just be for the identification, or would it provide any other purpose?

VOLKER GREIMANN: It would still provide certain other elements beyond accreditation, for example it would provide for a code of conduct, code of how data may be treated, a verification of the processes when requestor says that “I will need that data for X years to do that kind of fulfill my purpose.” The accreditation body checks that so there’s a code of conduct beyond identity, there's other elements baked into that that can be verified by the accreditation body that we would be able to rely upon as contracted parties, that we would not have to be checking for each and every single request, thereby releasing burden for us, but also releasing the burden for the requestor having to prove that every single time again and again, because that’s taken care of by the accreditation body, not the balancing test.

The balancing test is part of the individual request and the purpose of that request that is not part of the accreditation or the verification.

GINA BARTLETT: Thank you for clarifying. Mark SV, Stephanie, Thomas, and then Brian.

MARK SVANCAREK: Yeah, there's a lot to agree with in previous interventions. Within our caucus, we were thinking about the purpose of accreditation short of accreditation by a DPA as being useful insofar as it would allow us to test out some of these concepts. So Milton has suggested, what if there was just a series of direct contracts that would simplify this process? And we thought that might be a good thing to have in an accreditation framework even though it would ultimately not provide the same level of formality that would be provided by a code of conduct and a certified monitoring body and stuff like that. And we could use it as a stopgap on our way towards developing such a formal thing.

It would not provide the same level of functions, but it would still be useful because it would allow us to test our codes of conduct and our accrediting bodies as we’re going through the process of creating codes of conduct, getting DPAs to weigh in on these things. It wouldn’t be throwaway work even though ultimately – well, this is the sort of bet that we’re taking, is that it wouldn’t be throwaway work, that it would be useful work as we begin, even though ultimately, we would be working towards something more formal.

GINA BARTLETT: Thank you, Mark SV. I've got Stephanie, Thomas, and Brian. And any light you could shed on this question around the balancing test would also be helpful to build a bridge there.

STEPHANIE PERRIN: Basically, I agree with what Milton has said, and Volker and Allan, but I wanted to point out that I think we should not underestimate the cost of running various codes of conduct and accreditation schemes past the DPAs, because each industry association who cannot in themselves be trusted because there's the inevitable symmetries and asymmetries in an industry association, the competitors, they get along, they find a common interest which in this case is not coincident with the interests of the end registrant, it is in fact contrary to that end user.

So they would need to be each certified, and that’s just a huge amount of work. I appreciate Mark’s comment that it’d be interesting to kick it around, but we would certainly wear out our welcome at the DPAs if we came in with one for the cybercrime researchers and one for the trademark lawyers, one for the police and one for the administrative investigators, and the list could go on quite a ways.

And we mustn't forget that any individual has a right to inquire and go through this process, so that when we're building a system, it's also got to accept other or without restricting the generality of the foregoing, anybody can do it.

So I'm not sure. I think it would be very useful from the point of view of helping people understand the thought process in evaluating whether a request is acceptable, because sometimes I wonder if we're there yet, but it's going to cost a lot of money.

I would command what I keep saying from the time I showed up here, is ICANN could come up with a set of binding corporate rules with a well-spelled out policy so that we wouldn't be dithering around about how long you've got to keep the data. It'd be clear. That might be a quicker route. Also slow, you still have to get those things agreed by the data protection commissioner, but it has the same ability to bring in standards.

I just wanted to point out that ISO is cranking up 27001 again. I'm sure you all know that, but that's the only relevant standard. Thanks.

GINA BARTLETT: Thanks, Stephanie. Thomas and then Brian.

THOMAS RICKERT: Thanks very much. I think Stephanie, we should have another discussion about binding corporate rules versus code of conduct according to Article 40 and the duty of this or that. But I think we're moving towards getting align on what the idea of the accreditation and accreditation bodies would be.

I think what I'm hearing, and what I do support, that this is about identity of the requestor and the affiliation of the requestor, not about the request, where the balancing test exercise belongs to the request and not to the requestor.

And when we heard earlier, "Is it just the identity?" I think if we can confirm the identity and affiliation of the requestor, that's quite a massive achievement. You want to know whether somebody actually belongs to a certain profession, whether they still belong to that profession. You know you might have a retired police officer who's still filing requests for different purposes, so we want to make sure that we have an accreditation function that manages the accreditation of the individuals, that can withdraw the accreditation of individuals, and we want to be able to kick out the entire group of folks that belong to this accreditation body, thereby keeping the accreditation body in check that they have a genuine interest in playing by the rules.

I think if we can settle on these few parameters, we have something that we can be proud of for this early phase of the [inaudible].

GINA BARTLETT: Okay. Thank you, Thomas. I'm going to go to Brian and then I'll attempt to summarize on the purpose. Go ahead.

BRIAN KING: Sure. Thanks, Gina. A couple notes. You asked about the balancing test in particular. I think more in-depth conversations about that are probably premature until we get the legal advice we've asked for from Bird & Bird on that point.

I think one of the points that Stephanie made, I definitely agree. It’d be helpful perhaps to have the DPAs [bless] the framework here if we can get that. I don’t want to wait for that, but I certainly agree with here there; that would be helpful, but not the individual code of conducts or the parameters for each accreditation body at this point.

There are no approved code of conducts as far as I know, so we should not wait for DPAs to bless that for this to take shape. I think good in the future if different accreditation bodies explore that and did it for sure.

I heard a couple of thoughts form the NCSG which [I’d like to] invite to elaborate a bit, about the potential for abuse by someone who becomes accredited. We can't fix that. We can't guarantee that there will not be abuse of the system. What we can do is put sufficient legal parameters around who can be accredited, what they need to agree to, how that’s audited, and what happens when any abuse is identified.

We don’t want abuse in the system, and we need to have a system that works for those that want to use it appropriately and has the potential to identify and address when unfortunately abuse happens. But I'd like to invite any kind of constructive feedback on ways that we might be able to address, identify and fix abuse, but we can't poopoo this whole thing because it has the potential for abuse, like any system would. Thank you.

GINA BARTLETT: Before we go back to hear from the Noncommercial Stakeholder Group on that, I'd like to just see on the purposes, so what I've heard is that as Thomas put it, the requestor, the identification of the requestor, I think everyone agrees that that is a purpose of the accreditation system.

A second one that I've heard is a code of conduct, or it might be a series of contracts that define that code of conduct, but there's a body of thinking that is a purpose of the accreditation.

And then there's also a proposal that it might be an opportunity to spread liability. Where I don't hear agreement – and I think Brian just proposed that we wait until we hear what happens later, we hear from the Legal team – is how to manage the request.

I understood from Alan G that you were proposing that part of the accreditation system would be – the purpose would be the trust component which would speak to the request itself. I think I heard you say that. Maybe not. So I wanted to call on Alan G and Allan W to kind of help too on this piece around the actual request and how far we go with that with regards to the purpose of the accreditation. Could you clarify, Alan G?

ALLAN GREENBERG: I'm not sure, but ... As I hear things, we have people on the contracted parties side of this discussion, some of whom say “There is no way I'm going to give up my right to do a balancing teste on a case-by-case basis,” and I hear other people saying “There's no way I'm going to survive without some level of automation for some class of high-volume requests.”

I don’t think we’re going to change that. It has to do with their business models and the kind of business they're in, and I think we’re going to see that going forward.

So I think anything we build has to have an escape hatch that any given data controller who’s been asked to release information has to be able to say “I refuse to accept the automated path and I want to do it manually.”

So we’re not going to fix the problem that people have different needs, and I think we’re going to have to accommodate that particular one. So yes, some people are going to be willing to trust the balancing test on an automated – with or without artificial intelligence – and some people will not. And if we can't accommodate that, then we’re never going to leave this room. So let’s just accept that.

So from that point of view, I think we’re also talking a lot about how can we make sure that no one ever lies to us. We can't. How can we test things? Well, right now if Volker or Allan Woods would like to do individual balancing tests, you cannot test that any given subject will never violate the trust you're going to put in them by giving them information.

However, remember, in most cases, we have an obligation to report to the data subject that we've given out information. We’re going to have a large, complex process by which people can yell and scream and say someone’s not treating data properly.

I think ultimately, there's a lot of different components and they work to control each other.

GINA BARTLETT: Thanks, Alan. Allan W, and then I've got Stephanie and Hadia.

ALLAN WOODS: I suppose going directly to what Alan said, my biggest point about – we can accept that, absolutely. We can accept that – if we can accept an SSAD where the controller can turn around and say “I'm not happy giving data in this instance,” That’s absolutely where we need to aim for, without a shadow of the doubt, completely agree with you there.

The question is, is this group going to agree on that escape hatch? And that is a question. Well, yes, I agree. But it ultimately comes down on whoever is making that disclosure, on that controller, and we need to be mindful of that. So I welcome that, absolutely.

I had another point, but of course, in the grand scheme of things, it’s fallen completely out of my head. Yeah, sorry, I had a point, I just can't think of it.

STEPHANIE PERRIN: I must have misunderstood what Alan was saying with respect to escape hatches. I thought that meant that that was an escape hatch from treating each individual request as an individual request and thus following the law.

And I was going to say that the mere fact that my business model says I have to be at the airport in 60 minutes when it ought to take me 80 minutes to drive there doesn't mean that I have an escape hatch if a cop catches me speeding; right?

So people's business models are going to have to be altered to comply with data protection law, and I hate to restrict it to GDPR because it's cropping up everywhere, so we have to figure out how to come up with a system that has some flexibility into it, allows some kind of automation – because I'm well aware that we need some kind of automation – but the scope of what is requested in a first run can be nonpersonal, winnowing the field down to avoid how much work we have to do on the personal information requests.

Now, the other thing that I wanted to point out was there's a lot of – and the report was excellent that we got this morning or last night, but I'd just like to reiterate that once the data is out, no amount of insurance or redress helps the individual whose data has been breached. So that's why privacy is so hard and fast in terms of making sure you don't let it out.

We all know mistakes happen. That brings me to the point that caused me to raise my hand, and I guess it was in response to Brian. Yes, there will be abuse. The fact is insider abuse has been responsible for some of the major recent breaches. As a [inaudible] person who interrogated third parties on what they were doing with data, the final question was always, “And what are you going to do about insider abuse?”

And very few companies had adequate procedures for dealing with insider abuse. For making sure even that their security people were cutting people off when they left. And I was in government. I don’t need to tell tales out of school about what we did in government. You can read the auditor general’s report which regularly nails every western government that I know of for inadequate security procedures, particularly in the matter of personnel control and access to personal information.

It just has run along as a free rider and nobody paid enough attention to it. But now they get access to personal data that’s worth something on the black market. So I think that when you evaluate a candidate, company, organization, whatever, you can certainly demand standards for how they manage their personnel access.

But that means you’ve got to go in there and audit them. Thank you.

GINA BARTLETT: Thanks. I've got Margie, Thomas, and James. Oh, I'm sorry, Hadia was next, and then Margie, Thomas and James.

HADIA ELMINIAWI: It’s fine. I'm glad Stephanie mentioned automation, because actually, [I would put on the purposes] that in case we have an automated system or sort of an automated system, accreditation would be particularly helpful in this regard.

And we were talking about abusing the system. Well, this is always a possibility whether we have an accreditation model or not. So this part of the balancing test, in the morning I was saying – Thomas misunderstood what I said. He thought that I was saying that manual processing is always required. And that's not what I was saying.

I was saying actually that we could have an automated system, and we could do the balancing test each and every time, while automating this process, like automating the balancing test.

And maybe this is the point that everyone is dropping. Everyone is thinking it's either doing the balancing test manually or not doing it, because we have accredited user groups with certain predefined cases. But we could add to that element automating the balancing test. Thank you.

GINA BARTLETT: Margie.

MARGIE MILAM: Thank you. I was going to say something similar to what Hadia was saying, is that the balancing test – I'm looking at this as there may be categories of requests that don't require a manual review of the balancing test, and that's some of the questions that we're asking the legal counsel: is it possible to have an automated answer when you're dealing with a 6.1(f) example?

And that'll be a good answer. If the answer is no, then that changes where we go with the policy. But if it is possible to have an automated response in certain circumstances, I think that’s what -I feel we’d like to see.

Now, the other thing that I think we need to understand is that it’s not just 6.1(f), there are other legal bases that apply, and some of those do not have balancing tests. So I just want to remind everyone that there are other legal bases. We’re waiting for legal counsel on that, so we have to kind of think of that as we build this system.

And then the last thing, I just wanted to clarify that when we talk about codes of conduct, at least what I thought we’re talking about is contracts that track what a code of conduct would be. But as Stephanie indicated, I'm not sure the DPAs want to go blessing every single accreditation body, and I don’t think we should build a policy that does that. We should just kind of get approval of the overall framework and then let that be approved without asking for a DPA to approve every single accreditation. That’s not the role, and I don’t think that they would actually do that. Thank you.

GINA BARTLETT: James?

JAMES BLADEL: Thanks. Just to touch on one point that Stephanie made. I think you hear quite a bit from contracted parties about liabilities and legal exposure, but I think indirectly – and perhaps it needs to be stated explicitly that there is also a concern for the harms that could be inflicted upon our customers, the data subjects. And just because it’s not being said every time we make an intervention, I just want to be clear that that's not necessarily something that’s absent from our mind. I think it is baked into the concern that we have for the regulatory risk, because obviously, if we’re being held up to some kind of fine, then that means we did something wrong, and we probably harmed some of our customers in the process. So those are hand in hand. Thanks.

GINA BARTLETT: [inaudible].

[CHRIS LEWIS-EVANS:] Just sticking to the purpose section on this, I think Stephanie sort of went around it a little bit. One thing that we haven't had in any sort of disclosure and one thing that’s really important that we get from accreditation is the ability to audit the whole processing partway, so being able to say where breaches happen.

Without accreditation, you're not going to know where the data’s gone. So we have to have some accreditation of that requestor, how they were using that data, and to be able to audit that process, you need to have accreditation. Without it, you can't do that key function of seeing where that liability lies and who has caused the data breach.

MILTON MUELLER: What's the connection? So you say accreditation gives you the ability to audit? To my mind, it moves the auditing ability out of the

SSAD operation and into the third party who has nothing to do with the SSAD.

[CHRIS LEWIS-EVANS:] Who said the third party had nothing to do with the SSAD? That’s a possibility, but it’s not agreed yet. We've not –

GINA BARTLETT: So you're saying whatever accrediting body is agreed to, that this, another purpose of the accreditation system is to provide this pathway, a process so that you can track the data, but you're not advocating for who is the accreditor.

[CHRIS LEWIS-EVANS:] Correct.

GINA BARTLETT: I'm going to go back to Mark SV, and then I just learned that lunch is here so we need to break, so I'll go to Stephanie and then I'll kind of recap where I think we are, because after lunch time, [certain] is the Göran and the Strawberry team.

MARK SVANCAREK: Yeah, I want to make a similar comment which I think is in line with what Milton was saying too, that one of the purposes of the accreditation system is that there would be a monitoring body that would be tasked with doing such audits and hopefully the data controllers could trust that monitoring body.

As Alan says, maybe they come around and say, “Please trust us,” and then you evaluate whether they're trustworthy and then thereafter, that can play a role in the balancing test without actually imposing upon you the obligation to go and do audits, which is clearly not a practical thing for almost any company to audit another company. Thanks.

GINA BARTLETT: Stephanie?

STEPHANIE PERRIN: Thanks. It’s a bit late in my career to shift from data protection policy to competition policy, but I'm very worried about the concept that accreditation through industry bodies is the only way to ensure that there are good practices. Some of the best practices in Canada, when we were bringing the law through, were from organizations who refused to join for instance the Canadian Marketing Association. They had excellent practices.

You could go in and audit their practices and know that that company could be relied on, and they weren’t accredited. That would be the same here. So while I take Chris’ point that the idea is to lower the workload on the part of the organizations that are complying with the request, we also get ourselves into a whole mess of competition policy issues, cartels, all the rest of it, particularly in a global environment. Thanks.

GINA BARTLETT: Okay. So I think on the purpose, we agree that the requestor and the identification is a purpose, removing the burden from an entity providing disclosure, that there's a need to have a code of conduct of some type or a series of contracts depending on the method.

There's a purpose of potentially spreading liability, and there's also a purpose of providing this kind of process pathway that Chris just mentioned to track data monitoring.

The big lingering, remaining question is around the balancing test, whether it’s automated, manual, and the escape hatch, and that concept of the escape hatch is what I think I heard as a question.

I'm not sure I totally understand the escape hatch so I'm just trying to capture that, but the question around the balancing test and is that a purpose of the accreditation system, I hear differing views on that.

I'm going to keep going because we can keep talking about this after lunch, but we’re at a break, we have to break. As far as the requirements, while you were talking, I did pull out some requirements that might feed into the policy.

One is a requirement that the accrediting body is certified, but there's different points of view on how that certification process would proceed. Some are saying that it should be tied into Article 42 and 43, and it sounds like others would like that to be broader and that there be some other way of certifying the accrediting body, but there's a need to test the accreditation body so that you have confidence if you are using it, and it’s beyond – whomever it is or whatever it is. And then lastly that to manage for abuse and have an ability to subject the accrediting body that they could lose their certification.

So it seems like the question here is, who does the certification, or is the certification, what are the requirements, and then who can serve as the accrediting body? I hear differing viewpoints on that as well.

I think with that, we probably need to pause, but I've got Hadia, Chris, and Ashley, and then we'll go to lunch.

HADIA ELMINIAWI: Yeah, just a clarification. The automation part has nothing to do with the balancing test being automated or not. if we end up with an automated system, having an accreditation system will be beneficial in this regard. So it's not related to the balancing test or anything else. It's simply accreditation that's beneficial in case we have an automated system, even if we don't have an automated balancing test or none of that.

So I'm wondering why didn't you put it as a purpose.

GINA BARTLETT: I just misunderstood you and I can capture it. I understood as something different. So I'll rewrite that. Thank you. Sorry about that. Chris?

CHRIS LEWIS-EVANS: Yeah, just quick point of order. We haven't gone through policy and the who part yet, so we're not summarizing it. We've got quite a bit to say on that part.

GINA BARTLETT: Yes. Thank you for that reminder. I was just noting a few things that I thought I heard along the conversation, but we can pick up with that at the next point. Did somebody else want to get in? [inaudible] Okay.

JANIS KARKLINS: Thank you very much, and just one element that I wanted also to bring to this conversation, and maybe you can think about it during the lunch time. So there are two organizations mentioned in the conversation, and that was Interpol/Europol, and WIPO as a potential accrediting body.

So both of them are intergovernmental organizations, and that is different from industry association. So they have different legal status, they have different task, and probably, they will not come to ICANN saying we want to perform accreditation and vice versa. ICANN will go to them and will say "Would you agree to do accreditation?" Because they have a certain status in this game, so either we go to them or we will not have them as accreditation bodies. So that needs to be factored in in our thinking and conversation.

Different story is that if we do not have existing organization that could perform the function with a certain legal status, so then of course that's a different situation.

So with this, I think we can break for lunch. We will come back at maybe 1:10, that's one hour from now, and the conversation with the CEO will begin at 1:15. We will play the same – in the way that we've agreed. I would ask those questions that have been submitted already, and general one, how CEO sees the role of ICANN and in the system that we're building. We'll let CEO speak, and then we'll open the floor for any questions you may wish to ask as a follow-up clarification, or completely new questions that you wish to ask.

So we have one hour with him and one hour with the Strawberry team. 45 minutes. So with this, this meeting is adjourned, and bon appetit.

UNIDENTIFIED MALE: How long do you expect the CEO to speak?

JANIS KARKLINS: I don't think that he will speak more than ten minutes. I will ensure that he leaves sufficient time for us to interact with him and ask questions and provide or spell out concerns.

[END OF TRANSCRIPTION]