

---

**ICANN Transcription**  
**GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 1-PM**  
**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://gns0.icann.org/en/group-activities/calendar>

JANIS KARKLINS:

Good afternoon. Welcome back to the team meeting. If I may ask team members to switch gears and come back to the meeting room. We have a session with the CEO of ICANN, Goran Marby, followed by a session with the Strawberry Team. Elena will answer questions related to activities of the Strawberry Team.

Maybe using this opportunity, I would in three sentences describe where we are now in the process. We have gone through the deliberation phase by using use case methods and going through different real world situations that may occur and how GDPR would apply to those cases and draw on conclusions of that work. Staff drafted a zero draft as a foundation for our work here in the face-to-face meeting.

In essence, we're working on the hamburger model, since ICANN now is in food battles, we thought that that would be very appropriate to use. I had a chance to explain to you in essence what that is about, and I will not repeat it here to save time. In principle, the proposed model is accepted but we are far from

---

*Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.*

---

being in agreement on operational details of the system and how that may work. So we still have plenty of ground to cover.

With this meeting, we hope that we will be able to break through and then get some fundamental decisions on the shape of the system from an architectural point of view and [working on details]. In this respect, your presence here and [direction with] you is essential in order to understand the parameters that we need to factor in in our discussions.

In this respect, we formulated as a team questions that I sent to you. I can only repeat them here and see whether you are in a position to answer or give elements of answers to those questions. They are, can you please provide details on the liability ICANN org is expecting to take on in relation to reliability in a [inaudible] UAM? And can you please provide an update on ICANN's status on [as a] data controller or joint controller of domain registration data? In essence, that would be if you could outline maybe your vision, what shape the standardized system of disclosure and access should take.

After your intervention, then we will open the floor for any comments or questions team members may have.

GÖRAN MARBY:

Thank you for inviting me. If my voice sounds a little bit lower than usual, it's because I had the pleasure of spending the whole weekend together with my excellent Board for a Board workshop. Look how happy they look. Congratulations, by the way, for the work. There seemed to be a little [progress].

---

Before I start answering the questions, I want to take a step back just to put a foundation for how we think about it because I think it's good to know that. When GDPR came around, a legal risk was introduced. We already have a risk. Everybody who is in this system has a risk. So we have it. The contracted parties have it. The ones who gets the data have it. Everybody has that risk. So when you talk about the risk or liabilities, you should also figure out we already have that risk.

Someone said yes. When you talk about liabilities in that sense, this means that it's not that easy to define how you move risk when you already have it. This is extremely essential. We went out – I don't know if you remember – in 2017 and said we're some sort of controller. In the temp spec, we also said that we had some sort of risk. The problem is to define it all the way down because there's no [inaudible] anything about the risks – oh, sorry. The DPAs and the open commissions also said that we're some sort of controller. So we are not talking about shifting a liability. We're actually having a liability, but it's clearly undefined. We don't know how big that risk is. And we will never know until there's a court case of something coming around. So that is very important in this discussion: we're already under risk.

When we're actually talking about risks, there's a lot of talk about fines. You can talk about the probability: the risk that something happens and we have to pay a fine.

The second thing is all of this, which I think we talked about, is, when we did the first guidance we got from the DPAs – we're the only who actually got guidance. They gave us the right to collect the data. [inaudible] in the Phase 1 work was we had to right to

---

collect the data. We had to show some data, and some data has to be behind the curtain or something. That was the guidance we received.

Now comes the question, of course, of who gets access to this data? We put in the temp spec that we believe that the contracted parties have that legal responsibility. It's actually in the law. So however you try to do something with it, you always end up with the fact that the contracted parties always have a responsibility for taking the decision on who gets access to this data. According to the law, they have to make that decisions.

You're shaking your head over there. You don't agree?

Please explain to me how ...

UNIDENTIFIED MALE: Sure. With regards to the registration data, the contracted parties don't process that data for their own purposes. That data is for other parties' purposes and it doesn't seem to follow that they would be responsible for determining who could process the data or how it would work if they're not the controller, if they're not making the decisions around why the data is being processed, because the contracted parties have been clear that they don't need that data.

GÖRAN MARBY: I think other ones in this room might have a difference in opinion about that. If I may look at what the European Commission, who wrote the law, has written about it, they seem to have the same

---

opinion as we do. Let's state that we can have a difference of opinion, but that's the working [place].

The Board has given me, why is UAM done? There is a need [inaudible] that there is a need for this kind of data. Law enforcement, cyber security, and IPC would have need for this data. If you for a moment accept my way of looking at it, it means that then the only way to get a unified way of doing that is to [reveal] the contracted parties of their legal responsibility for giving out that data. Otherwise, everybody has to make that decision.

So, if you follow our assumptions, do you see the logic in this? Otherwise, whatever system that is set up, you always go to [inaudible]. The contracted party in itself has to make that decision. I claim it's not a bug in the law. It is actually the law, sustained then also by the DPAs, who actually asked us to come up with a model for some sort of unified access.

So that's where we are. I know you're going to meet the Strawberry Team. Why do I call it that? I got that question. Why do I call it Strawberry? It's because, if we were to do an acronym out of ICANN, it would have been [UAMBOTST]. I'm very bad at acronyms, so I had to write it down. That would have been the acronym for it. So I actually ended up just doing something more fun than that. You might not like my sense of humor. My team doesn't.

If you now see that the only way to achieve is to give the ones with the legal purpose the ability to have that information in a unified way, you have to build a UAM. ICANN's intention is not to make those decisions. I heard about your hamburger model.

---

---

Actually, [Becky], we can call it anything you can eat. We agree with the principles of that, with some smaller additions to it, like side orders. We'll do that in a minute.

UNIDENTIFIED SPEAKER: [inaudible]

GÖRAN MARBY: I don't know. I can't pronounce that word. There is one thing I'd like to reiterate about this. We are trying to figure out what is the missing point in this. All legal advice you get right now are opinions. They'll only be opinions that you get because the law in this area has never been tested. The European Commission – [hi], Georgios – has said that they are working with us, which is fairly unique, to formulate questions to the data protection authorities which are the ones who actually make the decision about this if this model is possible.

Elena and her team will talk a little bit more about what's behind that and what kind of questions we're asking, but that's the intention. That answer, when it comes back, has to go back to you guys. If the answer is yes, then you can make a decision if we should have a unified access model or whatever you want to call it. What [inaudible]? How should it be financed? Who should get access? Everything that is in that policy is up to you. That's not up to my work. If it's a no, then we at least know that there'll be no unified access to it. There could be a standard of access to it, when everybody uses the same sort of [key] to get access to the data, but the legal responsibilities will actually look like they do

---

today. We all share, to some extent, the legal responsibilities for it. The thing we're working very hard on at is that we don't get an answer that doesn't say anything to us. But it's actually up to you.

So see it in a way like this. Today it's a theoretical exercise about the policies, who gets access to the data, because we don't know. No one knows. If we get that legal guidance – sorry. The individual contracted parties – we might disagree – in my scenario, my little world of [flowers], are the ones that make that decision. We can't enforce something that is against the law. ICANN is not a regulator. So this actually gives the ICANN community, with legal certainty if we get to that, the ability to make policies around it because, when you have that certainty, you can start talking about this box.

As the background on that, I'm just going to spend two minutes on your questions. The first questions is really good, but it goes back to the basics that we already have a risk. Someone can utilize that risk today. We have accepted that risk. When we did the temp spec and decided we're going to have a policy – that is, you decided; when ICANN as an institution that WHOIS is a part of our DNA in the sense that it's in our bylaws and missions – we accepted that risk under GDPR. That's not a low statement. Then you can define how much is that. We don't know. That's the [inaudible] because there's been no caucus. But we have the risk.

If we then introduce a UAM – in our UAM model, which we will redefine according to hamburger, and that's what Becky's been trying to do over lunch, eating pizza – someone else outside ICANN accredited the requester of the information. ICANN works as a vehicle to ask the question to the contracted parties, and the

---

contracted parties have to ask that question back in the system. Then it goes out to the requester.

ICANN doesn't have the competence to validate or accreditate organizations into this. So that's why we reached out to organizations such as WIPO and Europol. As you know, they have other legislation things [than] GDPR. WIPO is a UN organization. Europol as a European institution is not under GDPR. They have other legislations.

So that is what we're trying to achieve, thinking that we already have the risk. We already have the potential and we need to figure out – that's one of the questions we're asking the DPAs: what will happen with the risk? We're a non-profit organization. We can't indemnify everyone in the system. The contracted parties have the risk today. By the way, they have many risks: other business risks, the risk [to make] business. We can't indemnify all of that because, basically, we don't have the money. You might think that we are a very large and powerful and rich organization. Compared to some of the companies that are present here, we are absolutely nothing. So the only way for us to build the UAM is also to make sure that we don't indemnify or take on someone else's risk. We can only deal with the risk that is not the mistakes we do.

Take the concept of joint controllership, for instance, which I know you talk about. Joint means joint. It's very interesting how you define that because it could be so that, if we have a joint controllership written down that you take on risks that we have – let's say that we have a data breach. We don't know, but how do you deal with that as a contracted party, for instance? If I do a mistake – I, of course, never do any mistakes in ICANN – and you

---



---

are suddenly liable for that, with 4% of your revenue? These are the things that we need to make sure don't happen if we create an UAM.

I hope that answers the questions about risk and liability. It's not a symmetric approach to this. It's more of a balloon. The law is also quite [inaudible] in that. By working through all the structures, you can actually limit your risk. I know that you've had some of those conversations this morning.

So we're trying to relieve the contracted parties of their risk when it comes to this. We are not trying to move that risk into ICANN. We already have a risk. We also think that there should be outside partners that actually take and validate the questions because we think that [these forces] are better at accrediting themselves rather than not.

If we succeed with this, it gives you an opportunity to design the policy that this could be based upon. That's not up to me. We're trying just to figure out the legal [order].

I open for questions. If you want to show our version of the hamburger model – if you have any questions before that. Ashley? I'm really bad at moderating, so, Janis ...

JANIS KARKLINS:

Yeah, I will take that. We have now a number of questions. Ashley was first, then Volker, then Milton, and then Hadia. Ashley, please go ahead.

---

ASHLEY HEINEMAN: Thanks, Goran. I have a question about what you said. I think I agree mostly with what you're saying. I'm just trying to get a little bit more clarity. I think everybody here recognizes there's no way ICANN can provide any kind of indemnity ...

GÖRAN MARBY: I like the sound of that, by the way. It's [very welcoming].

ASHLEY HEINEMAN: You can't provide indemnity for all the contracted parties. I think what at least I'm trying to corral in my head is, is there any way, if we're going to really have value and a unified access model and bring actual efficiency beyond what we're experiencing with the status quo, ICANN take a larger responsibility? In my little head, that is putting you in a position as ICANN to make decisions and conduct balancing tests and not make that a responsibility of the contracted parties. To do that, that would put some additional liability that you otherwise would not have.

Now, that's not the same thing as saying you're taking away everybody's liability, but it's also putting squarely on ICANN a responsibility for a processing activity that I think, if we ever got to the point of this being recognizable for ICANN and we recognize that you're able to take on that liability, that we can actually make some progress in these conversations. Thanks.

GÖRAN MARBY: Thank you. I refrain from the word "processes." The reason I do that is actually because, when I speak to the European

---

Commission, which you know we do – you can always ask Georgios about ... sorry. I have a problem pronouncing his name. Therefore – yes, I know – that it comes out as “Gorgeous” every time. So, please, he’s gorgeous, so it’s not a lie. But I feel a little bit ... Here’s the thing. We already have a risk. So look at it from this perspective. We have a risk. What are the [inaudible]? 4% of 2-something. That is the [inaudible]. Now we can go down how that is calculated. But let’s accept that as is. So we have that. If we add something to it, the fines are still the same. The probability might change, but the fines are always the same. So it’s hard to say, yes, you do this and you actually increase because it can actually be, as you do something, you actually decrease it because now you’ve designed a process for doing it. One part of the law is that you actually design the process. So it’s not like you move one risk from one place to another. Everybody has to have their own risk.

The other thing is that I think that ICANN would have a problem to do the balancing tests. I think it’s better to have police forces and other ones who actually know the law. That’s why we’ve spoken at length for a long time with Europol, for instance: they know which law, how to do it, and they can be aggregator of police forces because, by the way, they said they were interested to do it. So we will provide the mechanics for them to be able to do that. Same thing with WIPO. We’re actually looking for someone who could be accredited. The problem that I [inaudible] accreditation is actually because it’s in the law that you can have that status, and that can only be assigned by the actual government to do that.

---

But that is the model we think should be working, and that's the model so far, it seems, a way [inaudible] because I truly do not think that we are capable of doing that balancing act. It's not about the risk, per se. it's more making sure that we actually have the right answers to the question. And [we'll] put ICANN as an institution to validate the police – if a police force comes in with a request, it could be hard for us to validate that.

ASHLEY HEINEMAN:

I'm sorry. I just think it's really important to make one clarification here because I see lots of heads nodding and I think there was a misunderstanding here in the question. It wasn't so much balancing with respect to accrediting entities. It was when you're faced with a request for information. Right now, the legal basis basically requires whoever is making that decision to do a balancing test. It's whether or not ICANN, as the meat of the hamburger, is willing to take on that kind of responsibility.

So what I heard you say is a bit different from what I asked. I'm happy to take this offline, but I just want to make sure, when we have conversations later, that we don't wake away with a misunderstanding because I did see a lot of heads nodding but that wasn't exactly what I [meant].

GÖRAN MARBY:

I think or intent is the same. Our end result is the same. That's why we are engaging with the European Commission and, in the end, the DPAs: to get answers to those questions of what can do

---

what. Remember, this is an assumption that we're making based on input from the European Commission and the DPAs. So we made an assumption and now we're going to try to the assumption. It could be wrong. Then we have to figure out a Plan B or a C or a D or whatever it's going to be because remember the other side of this. There's a big interest from law enforcement from intellectual property – [now I got it right] – from cyber security access to get access to this data. There are still unknown questions, like when you talk about risk. If someone gets data – let's take cybersecurity, to pick on someone else for once – and deemed to be that you got that information the wrong way, you're now under GDPR and can be fined. So it's a virus in that sense. The fact that you have the data in your possession, regardless of your restriction, creates a problem for you.

I don't know. Do you want to do questions or Becky's hamburger?

JANIS KARKLINS:

I think we should not take anything offline. This is the unique opportunity, and probably the next time we will have in two months in Montreal and probably not as generously as now. We need to squeeze out everything from the CEO during this session.

GÖRAN MARBY:

First of all, my name is Goran. And squeezing is not something that I appreciably like. To your point, I will make myself available every time you want to talk to me, as long as it's not in the middle of the night.

---

JANIS KARLKINS: Thank you. I will take Volker, Milton, and Hadia, and then we'll go to Becky and then we'll continue with the questions – no, we'll continue questions. Everyone will speak. Please, leave it up.

VOLKER GREIMANN: Thank you, Janis. Thank you, Goran, for your words. I agree with a lot of what you said. However, one thing that is clear to me at least is that we had a certain risk that has been largely mitigated by the temp spec. If the temp spec hadn't happened, the registrars probably have mitigated it on their own by redacting the data in some form or shape.

GORAN MARBY: Do I hear a thank you in there?

VOLKER GREIMANN: I'll give you that. It's just now we're talking about reintroducing risk by making that data more available again to parties that want access to that data and mitigating that additional risk that we're now creating. So when you're saying that there is risk already, then you're right, but not completely right.

GÖRAN MARBY: I think that we have to totally agree. What I'm saying is that, when it comes – well, first of all, we have a risk. But it's hard – I think we agree – to say exactly how that risk will work because it's not a [fight in court]. So the acceptance of risk is important.

---

The second thing is that I agree with you. You have a risk every time you leave out the data. Janis, don't say that you said it before, but I have said that before for the last two-and-half-years: that the whole assumption with this is that I think that you have that risk. You disagree, and that's fine. But I agree with myself. That didn't come out the way I meant it.

So, so far, we don't have any disagreement. I think that you have that risk. The whole point is for us as ICANN to mitigate your risk. We're trying to do that. But I never said I will be [inaudible]. I actually gave you a promise about the first guidance we got. I gave you a high level of probability that we will get something and it will be good. Some of you didn't believe that, but we got it. It was hard work and it was thanks to the ICANN multi-stakeholder model that we got that. Otherwise, we would have got nothing. So you're right. We're trying to mitigate that risk on a central level. So we don't have a disagreement, but thank you for the compliment.

JANIS KARKLINS: Thank you very much. Next is Milton.

MILTON MUELLER: First, just as an informational thing, we've been having some fairly sophisticated discussions of accreditation. I would let you know that the concept that you're floating here – throwing off a lot of responsibility onto WIPO or INTERPOL – is not really where things are going to go. It's not going to solve the problem you think.

But that's not my question. My question is—

GÖRAN MARBY: Milton, can I ask you a question? Just for me because I haven't been in the conversation.

MILTON MUELLER: Okay.

GÖRAN MARBY: You used the words "going to throw away a lot of responsibilities to WIPO and Europol." What do you mean by responsibilities? Is that a legal responsibility or is it something else?

MILTON MUELLER: I mean responsibility for proper use of the SSAD or what you call the UAM so that the fact that INTERPOL decides that somebody is a law enforcement agency will not absolve the system we're designing from the need for auditing and enforcement of proper use of the system. It sounded to me like you might be thinking that you would dispose of that problem by pushing it off to WIPO and INTERPOL. I could be wrong, but that was just a heads up that we are having fairly sophisticated discussions of that problem.

So the question. I'm really running around in circles trying to make sense of fundamental issues that you're addressing. It seems to be me you're saying three different things, one of which contradicts the other things. You say liability is unknowable until there is a court case, which is probably correct, although we can have some sense of what's legal and illegal and we designed the



---

temp spec and the initial policy around that. Then you say liability is already there and cannot be shifted around—

GÖRAN MARBY: Milton, a small correction. We created the temp spec based on the guidance from the DPAs.

MILTON MUELLER: Exactly, yeah.

GÖRAN MARBY: I think it would be very hard to do it otherwise.

MILTON MUELLER: Right, but we probably had a pretty good idea of what was legal and illegal when we did that, right? So let me finish the question here. On the one hand, you're saying the liability is already there and it cannot be shifted around, which is a statement that has some coherence. I think I know what that means. But then you keep saying we should relieve contracted parties of risk by creating a UAM. So I don't understand the connection between those two statements. It seems that they directly contradict each other. Either we're relieving the contracted parties of some kind of liability or risk by creating the UAM or the risk is there anyway and the UAM doesn't make any difference. Maybe I'm just dense, but I just don't understand how these things are ...

---

UNIDENTIFIED MALE: Please use microphones.

GÖRAN MARBY: Milton, I can answer this. If we agree that the contracted parties have a responsibility according to the law ... sorry. If we agree on the fact that the contracted parties have the legal responsibility and obligation that, every time they get a request today, they have to make all those balancing [tests], then that provides a legal risk for them, which means that 2,500 contracted parties in essence will deal with that differently.

You don't believe that?

Thank you. Which means that, if we can relieve that of that legal obligation, you will have one way of dealing with all the requests and you can know how you get the answers.

JANIS KARKLINS: We need to use microphones, Milton.

GÖRAN MARBY: So you might be right. I'm not saying that you not might be right, but that specific question, instead of you and I having different opinions, is the question we're trying to ask through the European Commission the actual DPAs.

MILTON MUELLER: Right. I'm really not trying to catch you. I just want to make sure I understand what you're saying because, if on the one hand you

---

say you can't shift the liabilities, it seems that that's precisely what we're trying to do by creating a unified system.

GÖRAN MARBY: No. We already have a liability, which means that, if you look at, the liability [inaudible] goes up. We already have the liability.

JANIS KARKLINS: ICANN org, probably.

MILTON MUELLER: Yeah, who's we? You're saying on one hand it's the contracted parties. That's what I thought.

GÖRAN MARBY: Okay. I think we'll [proceed].

JANIS KARKLINS: Let me take Hadia's question, and then, Becky, you will present the chart.

HADIA ELMINIAWI: Thank you, Goran, for being with us today. Based on what you just said and going back to Ashley's question about decision making and looking at the unified access model that was proposed by the Technical Study Group, what I see here is that actually, as Milton said, we've been talking about accreditation entities. What seems doable now is that maybe the accreditation

---

entities would also validate the questions. That is, the accreditation entities would also make the decisions. Is that a possibility?

GÖRAN MARBY: Definitely.

HADIA ELMINIAWI: And that reduces the risks that lie on the contracted parties because the decisions are made by another entity. If the answer is no, I still do see a merit in doing that because this whole decision making process will be done by another entity, and thus the contracted parties would not need to invest in this regard.

GÖRAN MARBY: Correct. You say it better than I do.

JANIS KARKLINS: Okay, thank you. For the moment, we are explicitly calling two organizations by name, and that is Europol or INTERPOL and WIPO. But we have categories of potential requesters that would not fall within the remit of neither law enforcement nor intellectual property. There isn't, at least at first glance, an obvious organization that would do the job as potentially WIPO and Europol who do law enforcement and intellectual property. So probably we need also slightly more details on what these other organizations could be, or we need to create them.

---

GÖRAN MARBY:

In the law, there is a potential for the government to accreditate an organization. If you look at [our friend], [Sinak], who consists of governments, who seems to have an interest in that, it actually could be a question to them because it's an individual country because of the motions of setting up an accreditation body. I'm [sword sliding] many laws and many discussions in this one. There is an excellent guidance about this in the DPA Board on how to do this.

JANIS KARKLINS:

Thank you. Becky, if you could.

BECKY BURR:

Is this on? Okay. This is just how we understand the hamburger model. The picture is a little small, so I'll leave it up here. Outside of this model, you have a whole bunch of policies. That's the work of the PDP, which is coming up with rules that say, "This kind of person should have access to this data for this purpose." That's the policy that you get. You have all of those.

So you have a requester down here – the bottom bun – and a place where the data is stored for purposes of providing access to registration data. That same data may also exist for other purposes like billing and stuff. That remains on the contracted parties. But what we're talking about here is accessing data for purposes of providing access to registration data.

In this picture, you've got the burger or the TSG/UAM in the middle, and then you've got all these condiments on the side. You

---

have to pick one of the condiments – so with WIPO or Europol or mustard or lettuce or whatever.

So the flow is – I’m going to preface this to make sure we’re all on the same page here – that a requester comes in and says ... First of all, a requester has gone out and established its identity and its bona fides with one of these condiments, and it has been deemed by the condiment to be in the category of people who are entitled to have access to X data for Y purpose [inaudible]. So it comes and says, “Here I am. Here’s my credential that says I’m entitled to this data for this purpose. Please give it to me.”

But UAM takes the request and goes over to the appropriate condiment and says, “We have this token. Is this person who they say they are, and are they in the class of people who should have access to X data for Y purpose?” If the condiment says, “No. Stop,” they’re not entitled. If the condiment says yes, then the TSG sends the request up to the repository and says, “We have Person X with Credential Y who’s requested data. We’ve gone to the condiment and authenticated their identity and their credential. Please send the data.” The data comes back down through the UAM to the requester.

The concept is not here and not there – well, maybe in there. They’re going to have responsibility and liability for the way in which they use the data, and contracted parties would have responsibility and liability for the way they use the data for billing and other purposes. But within this loop, the point would be that, for processing this part of it, the repository, the data holder, the contracted party doesn’t have the liability. That’s what we understand the goal of this process to be.

---

We heard some versions of the hamburger that mix the condiments in, and we just want to pull it out to make sure we're all on the same page about it.

JANIS KARKLINS: Thank you very much. Next let me ... we have many. Let me take Stephanie first and then Alan.

STEPHANIE PERRIN: Thanks very much. First comment is I think we have indeed had legal risks since ICANN was formed, and that came with reputational risk. What we have that is new is we have financial risk because there is a commitment to enforce and to fine. So that's the new element, not the actual legal risks that we've always had.

Secondly, I don't understand how you can ever absolve the data controllers or processors of their liability if you outsource the disclosure instrument to parties that may not be independent and balance the rights of the individual appropriately against their own defined policy biases.

WIPO is interested in intellectual property protection. INTERPOL of course is set up by governments to do serious criminal investigations. That's an easy one. You won't get an argument from me on that one. But that does not cover very much turf in terms of what we're talking about in access requests.

So all these other requests – we can't just muddy the waters by calling them condiments. They are going to be the cybercrime

---

researchers, the independent ones, the telecom authorities, the ISP associations, the Save the Turtles – that’s my favorite for the day – defense leagues. There are all kinds of administrative laws kind of things that don’t fall under criminal law that are nonetheless extremely important.

So I don’t see that this model scales. It’ll cover the two easy ones, and then there’s this basic legal question of, can the contracted parties just sit back and say, “Oh, they made me do it. I outsource to a non-neutral party to make these decisions”? I don’t think that’s going to fly in court because they are the ones with the interface with the individual. So they still have a – I’m not a lawyer. Remember that. I won’t use the word fiduciary here because Becky will probably correct me. It’s not an appropriate use of fiduciary. But they do have the relationship with the customer. Unless you’re going to put it all in contract, force them, and then remove all the liability to ICANN through ICANN’s contract setting mechanisms – the same as ticket [sense] and all this that I complain about all the time – I don’t see how this works.

Anyway, that’s enough from me. Thank you.

GÖRAN MARBY:

I have no more comments than I said before on that since that is exactly the questions we are going to the DPAs with. I don’t know the answer. You may be right. I have no idea, but I’m asking the European Commission to help us answer those questions to the DPAs.



But I will pick on something: turtles. I like that one. Yes, it is. When it was decided that GDPR had an effect on WHOIS, there are individuals or organizations that [do] have access to the data. One of them is actually individuals. I often use the WHOIS to go in and check. If someone sends me a link about something and I get a bad domain, I go in and look at it. So me as an end user is using that. I'm probably nerdy, but I use that to validate. If it says Donald Duck there, I know it's probably not Microsoft. Did I break any intellectual property law by saying that, by the way? I got nervous.

So we're working [inaudible] strategies. We're trying to see if it's possible. The answer might be no, it's not possible. Then I agree with you. We are talking about a limited set of that information, but the problem is that I can't indemnify the contracted parties. We don't even know if that's possible, by the way, because, when we speak to legal (same as you sometimes), we don't know if we can actually take over someone else's risks. In that sense [we're] a contract, which means that we still end up – you seem to [inaudible], but if I look at the some of the contracted parties, how are they going to react on the questions about the turtles? You have that problem in every model that we're trying to build.

So I have no disagreement. Let's work it out and see what we can do. Our intention is not to drag this out anymore.

JANIS KARKLINS:

Thank you. Alan?

---

ALAN WOODS:

Thank you, and thank you, Goran, as well for coming. I know it's a particularly difficult room to sometimes talk to. I have three points, and I'll go through them briefly. I don't want to go into the – thank you, Margaret. I mean, three points is not enough now? So I don't want to go into the weeds too much, but I suppose the first thing is, when we're talking about the establishing of the liability, I think we need to be very clear that – you're right – until we go to a court and a court establishes or a DPA establishes where the liability rests, we're never really going to have that answer. But we do what we can and best approximate where we believe as a group that that liability will rest. That's what we're doing at the moment with ICANN/contracted parties. We're going through the data mapping exercise, and hopefully that will come dividends to that. Then we can probably have a bit more of a – I suppose at the moment we're trying to throw things at the wall and hope some of them stick, whereas, when we go through that process, we'll be able to make an educated guess. That's also going to be a legal educated guess to where that is. So we're working on that and hopefully that will give fruit to us at the end of that.

So that's my first point. We are working on that. The second one – again, this is potential going slightly into the legal aspect – is I'm very intrigued as to the statement that we have an obligation to disclose the status because I would firmly disagree with that very simply because, if we had a legal obligation to disclose the status, then this job would be so much easier because we would all rely on 61C. 61C is where there is a legal obligation to disclose this data. But the problem is we don't have that legal obligation. It is an expectation that we may process the data for such reasons, but there is no a legal obligation to—

GÖRAN MARBY: Did I actually use that word? Because—

ALAN WOODS: Yeah.

GÖRAN MARBY: [inaudible] say it was legal obligation.

ALAN WOODS: You said we have an obligation, yeah.

GÖRAN MARBY: Yes, but that's different. It's different to have an obligation as we've seen in the [inaudible]. Let's take a step back. The WHOIS system is a part of our mission and [bios] because that's what your founding mothers decided. So when I refer to that to give that information out as much as possible, that is – when the Board said, when we took the temp spec, "Who is this important to? It's needed for dah, dah, dah," we always accepted it. So, no, the problem is that we are not defined according the law as a public interest. We are defined as I don't know what. We're not even defined. If we were defined as a public interest, this discussion would have gone away. But unfortunately, that didn't work. So no disagreement.

---

ALAN WOODS:

Okay, great. Thank you because it was of a slight worry to me. It would be great if we were – obviously I agree – if there was some sort of a public interest. It'd make our jobs a lot easier defining that. But I will say, of course, as the Phase 1 – we did define what the purpose of WHOIS was, but again, we do have that open question on the dreaded Purpose 2. That's something we'll have to come back to.

My third one is again just taking up on something you said as well, and that's specifically with regards to these condiments and Becky as well and what you were saying: that the condiments would make the decision. So you're saying that, if they're accredited, they would be able to then say, yes, you could access to that data, which of course would be taking the control away from the controller, who in law must make that decision. So we need to be clear on that one as well.

BECKY BURR:

The final word is yet to be written, but at the very least what they're saying is this person is who he or she says he is and, based our review, they are in the class of people who are entitled to this kind of data for this purpose. So that's slightly different.

ALAN WOODS:

That is a slightly different take on that. I appreciate that. Thank you. But I will just add onto that I think, again, when we're breaking down the legal bases for the ones that are not 61F, I think that is actually a pragmatic potential way of looking at it. The problem is where there's that requirement of the balancing tests.

---

We're back to that. Again, I would just emphasize that the balancing test is a requirement to be done by the controller and not by the third party as well. Again, these are things we need to take into account when we're doing them.

GÖRAN MARBY:

Alan, right on every point. But I also think that we're in a way going down into the weeds. We are now in the process of trying to get some principle answers. The easiest principle answer – we have a UAM based on the TSG. The TSG based on a technical idea. The Strawberries are working around the legal basis. Then it's time to go and check if that's possible. But the answer might be no. Then my question back to the governments that says that we should be doing this because it's so important is, "Okay. How are you going to address it?" So we are doing what we are supposed to do. I trust the policy making process [inaudible].

But it could also be so, which I'm fine with – I could think about some other problems – that we find out the legal basis for a unified access model and you guys say, "No, we're not going to do that," which, in my role, that would be perfectly fine. But that doesn't have to be based on "We're guessing." It would actually hope to be made on "We know." That's the difference. This is the first time, but I don't think it's the last time ever, that we're going to do ... As not being a regulator to the policies we're making, all the contracts we're making, we have to base them on some sort of law, despite if they're contracted positions or they are policy made. We've always been there. I haven't been around that long, but I think this is the first time we are so contained in detail by a law. This is an exercise for all of us.

---

I pledge my commitment to this model, saying that we're trying to figure that out. If it's wrong, I think we have another problem because I also think you think, because you have decided as the multi-stakeholder model, that access to this kind of data about the transparency about the end points [of] domain names seems to be vital for security and stability. That's what you said through the bylaw submissions. You might as individuals not always agree with it. When I was here a year ago, I said my life would be much easier if we actually had a policy for privacy. So that's the [dream].

Next one.

JANIS KARKLINS:

Thank you. Next one is Brian and then Alan.

BRIAN KING:

Thank you. First, thank you, Goran, for coming. We really appreciate your engagement here and answering the questions. And thank for Becky for coming and for walking us through the alternative, very similar hamburger up there.

I may have follow-up questions depending on the answer to this question. I'm a little confused or maybe I misunderstood. Goran, earlier you said the contracted parties have to make the decision around disclosure of the data or access to the data, but the way I understood Becky's description of the hamburger there was that, if the requester was authenticated or validated or you name your verb by one of those condiments, they would be entitled to the data and, by submitting the request, they would get the data. I

---

didn't hear a processing step in there where the contracted parties would get involved or make any kind of decisions.

So did I misunderstand one of those two approaches, or what's the difference?

GÖRAN MARBY:

One is probably describing what we have today, which is not the hamburger. What do we have today? I don't know. [inaudible]? The hamburger, which is sort of funny – I personally enjoy your description of it – is the model we're trying to build. We're going to use the hamburger from now on. Look how excited we all look like. So this is the scenario we're trying to build on.

BRIAN KING:

I appreciate you clarifying that because that, I think, eliminates my follow-up question. But I'll make the point anyway that the economics do not add up to disclosure, even in many of the most egregious cases right now. There's just simply not incentive from my contracted party colleagues to ever give up the data right now. It doesn't matter what's going on on the website. They're worried about finds under the GDPR for giving up the data, and there's no incentive from ICANN or from anywhere else to process the data. So that cannot be the outcome that we have at the end of the day. Thank you.

GÖRAN MARBY:

[All right]. This seems to be the debate you have between you guys.

ALAN WOODS: I just want to say on the record that we don't need an incentive to do this. We're all sitting this table because we recognize that there is a need here. We're not here saying, "No, we're not giving to you. Convince us." What we're saying here is we're all trying here to figure out what the easiest way to do this. So to be perfectly honest, I don't think that's a particularly fair representation of our intentions at this table.

Sorry, I didn't mean to interrupt the flow.

JANIS KARKLINS: No. For the record, that was Alan, for those who are listening.

BRIAN KING: Yeah, and this is Brian for the record. No, I did not intend to imply any lack of good faith or anything along those lines. But I would point out that there are thousands of registrars that are not at this table that simply ignore all requests that we send to them and don't even acknowledge receipt of them. That systemically is not an acceptable outcome at the end of this. I appreciate our contracted party colleagues being here and working so hard on this. They work just as hard as any group here, and that really is noted and appreciated. But there are many of their colleagues that do not share that. So I just want to make that point. Thank you.

JANIS KARKLINS: Thank you. Alan, now it's your turn.

---



ALAN GREENBERG: For the record, Alan Greenberg. The previous intervention was Alan Woods.

JOHN JEFFREY: Can I put fingers on that real quick?

ALAN GREENBERG: Only if you give us your name.

JOHN JEFFREY: I will. I am John Jeffrey. I just had a question about that. I understand what you're saying and I understand that the incentives, if that's the right term, are hard. But shouldn't that be part of what you're talking about in here? Because I think the model is to create a model that works and is able to produce that information under certain circumstances. What it felt like when you were having that dialogue with Goran is you were looking at him and saying, "Why aren't you fixing this? Why aren't you giving us the proper incentives?" But I think that should really be part of this policy discussion, right?

BRIAN KING: Yes, I agree entirely. I just wanted to be clear that Goran wasn't saying that it was a presupposed outcome that the contracted parties had to be doing the processing. I just wanted to be clear that that's what we are on working on here and that org didn't feel differently about that.

---

JANIS KARKLINS: Thank you. Alan, finally. Alan Greenberg.

ALAN GREENBERG: Thank you. It's just amusing. When we started this process when some of us were very naïve on GDPR, there was a proposal that ICANN was a sole controller and that registrars and registries were just following the instructions given by ICANN and were processors. It dawns on me that, if we had decided that and put that in Phase 1, our life right now would be a lot easier. But for various reasons, that was fought tooth and nail, and that isn't where we ended.

GÖRAN MARBY: Can I make a comment about that? This actually goes to one of the hearts of this discussion. We might decide that. You and I might agree. But that doesn't mean that's the reality, especially since the DPAs actually in the guidance to us actually said we are all some sort of controller. So it's hard to [inaudible]. I don't know if you know what the word "guidance" actually means in this.

May I just explain that for a second? Because I think this is important. When we speak about guidance from the GDPR perspective, you have to think about the fact that the data protection authority or any authority in Europe cannot give any advance notice about something they're going to do, which means they can't have an opinion. Some DPAs have had opinions, but that's very unusual and very rare. But legally under GDPR they can't do that. But they can come together under the Data

---

Protection Board as a collective and they actually issue what is a formal guidance. By tradition – this actually works the same way as the thing I did before when I was a telecom regulator and head of that Board – that guidance stands up in court. It becomes a legal guidance. That also [prohibits] all the individual DPAs in Europe to have a different viewpoint on this.

So I just want to put that word “guidance” so it’s not a soft word. It’s a fairly hard legal term. Thank you. Sorry. Now, Alan?

ALAN GREENBERG:

As I said, I was musing, if the word had turned out differently, our life might be easier. But it was just a musing, not a proposal that we go back there.

My real comment is on reliving contracted parties and controllers of their liability or transferring or limiting or whatever the word is. I’ve heard words from our friends in the European Commission, saying, if we go to the data protection authorities or the board and say, “How do we relieve or move liability?” we might as well be speaking to a brick wall for the rest of that discussion. Somehow, the question is, how can we assume the responsibility – I’m sure I’m getting the words wrong – for protecting the privacy of the registrants while being allowed to make the decisions?

I still am hearing words of relieving and moving. As I said, I think I’ve head us being told that, if we use those kinds of words and verbs, it’s never going to fly. So I’d like a little bit of understanding.

---

GÖRAN MARBY:

I can now turn to Georgios. What's your second name? Hang on. Mr. Tselentis is over there, but I won't. Instead I would say that the European Commission, the three different [inaudible] [Home, Justice] and DG Connect are all engaging with us to help us to ask the questions. They also know that the only way, because they said so, to produce a unified access model is to take away the legal responsibilities. I'm not going to go – because it's going to be a very long sentence. When it comes to a question that goes to them, the question goes back.

So to take away your – remember, we actually did formulate the questions quite nicely because we got guidance. But this time we're actually going together with the European Commission to ask those questions. The European Commission has stated publicly in the GAC, in here, that they are engaging. When the Strawberry Team gets to their point, they will talk more about the structure and the questions themselves.

JANIS KARKLINS:

I will take now Greg and then Margie and the Chris.

GREG AARON:

Thank you. Is there an idea of how long this process is going to take to talk with the European Commission and get responses back? The dependencies are important for us because we may not understand what our options are until and be able to make certain decisions until those answers come back.

---

GÖRAN MARBY: The minute I go out of here, you're going to engage with the team that sits behind you. They are in charge of the time plan for it. But we have no intention of drawing this out, but we don't control the end result in that sense. But I don't know. The other ones will talk more about the timing of it. I hope that's okay.

JANIS KARKLINS: I think we will take it [after].

GREG AARON: It's a big work plan issue for us because, until we know the answers, there might not be things we can do or decisions we can make.

GÖRAN MARBY: We are totally aware about that, but we also talk about governments. Sorry, Mr. Tselentis. I'm guessing a second because I can't really see. But it's gorgeous and talented. That's what I see.

JANIS KARKLINS: Margie, please?

MARGIE MILAM: Thank you. I think Greg asked a lot of the questions I was going to ask. But one of the things that I noted from the European Commission letter was a reference to ICANN in offering the WHOIS in the public interest. From your perspective, are you

---

seeing that as -- obviously, Georgios can maybe answer that question as well. What does that mean? And does it have any bearing on whether the other legal basis we've been talking about could actually apply, which would mean that the balancing test won't necessarily always apply? So I'm just curious if you guys have been exploring that angle.

GEORGIOS TSELENTIS: Margie, to answer what you are asking there, in order to have ICANN acting on the public interest, we need to have some sort of legal framework or treaty or something behind this or the specific organization. So we are also looking at this and how this could be interpreted in this sense. If you are trying here to have ICANN having a role which is serving the public interest, then obviously it's not enough to have it in the bylaws. These are bylaws of a company under private law.

So there are several ideas that we would like to explore in this sense. There are possibilities, but I would say, if we go the hard way, which is to make a legislation, this, I think, will take us, as Goran said – governments have their own pace – some time. It might give a solution to a part of the problem, so we could use as a legal basis not the difficult ones but the balancing test. But it doesn't solve the problem of a timely deployment of unified access model.

So it can give us help and not necessarily solve many other issues that we're examining here, like accreditations and other stuff. In terms of hard law, it will take also time.

JANIS KARKLINS: [inaudible] Margie [inaudible]? Okay. Next is Chris and then Thomas. Those who have spoken and have not put their name tags down, please do it so that I see who is asking for the floor. Chris, please?

CHRIS LEWIS-EVANS: Thanks, Janis. Goran, can I take you back to your point on accreditation here? You said you didn't feel like you could be responsible and you weren't confident enough to become an accrediting body. I would suggest – this is probably a question for you – that you probably, as a data controller more responsible for disclosing the data, you would be best placed to be the accrediting body. If we look at your model with the condiments, if someone wants to put tartar sauce in a burger, not anyone would want that. So someone has to accredit the accreditors.

So really what I would hope that we can give you is the safeguards needed to be able to properly accredit different bodies and, between ourselves and the implementation team, the right policies and the right frameworks to give you that. Then I think you become an overarching accrediting body. You go to DPAs. You get Article 43 signoff.

But I think you're right. You're probably not best placed to then [say] the IP people and everyone else – so you could then contract those parts under the framework and the policies that we would generate for you. But for me, that's you taking on that responsibility for setting up a proper accreditation process that is

---

well-managed and within the lines of the policy that we're generating.

So that would be my ask of you.

GÖRAN MARBY:

So you represent the GAC? Thank you. You could fix this in a swift, very simple – because, if the 28 member states (maybe 27 this week?) ... At the same time – sorry? Yeah, whatever. Halloween, isn't it? I have not made a joke about Brexit in 24 hours. That was not true, actually. Yeah, you're right.

UNIDENTIFIED SPEAKERS: [inaudible]

GÖRAN MARBY:

Yeah. Being with you feels like an eternity, Chris. That's why – no, I'm joking. Because, as you know, if the European member states come up and accreditates ICANN as a –now we're not talking about the technical one but actually the legal ones, but the individual member states have to do that. We have deemed it a little bit hard to convene the 28. I actually once actually asked that question to the GAC: what are all the European countries coming there? I said, "Can't you fix this for me?" because we need a legal basis for the accreditation. If we become an accrediting body, we can do all that. It's hard for us because according to law you can't just be an accreditation house. It has to be done by a legal act. But the good thing is that it's inside the legislation that an individual country can do that.



---

The question also is what happens if one country actually does it – will it work as an accreditation in the other countries as well? We don't know that. It's a very interesting question which will probably solve the turtle problem. But then we have another legal status than we have today. So you're in the GAC. Come back to me when you talk to your colleagues. I don't want to be condescending, but that is the legal basis for it, sort it. I think I [inaudible] the Data Protection Board that actually issued official guidance, which you can find how this could happen. [inaudible] going to be in all our explorations. That's one of the things we try to explore during this very long process.

JANIS KARKLINS: Thomas?

THOMAS RICKERT: Thanks very much, Janis. Hi, Goran. Thanks for answering our questions today. While it is true that probably clarity on some of the questions that we have will only be given by court at some point, some things that I guess we can do and a lot of what GDPR requires is documentation, being transparent about internal processes and how personal data is being dealt with. I think that a lot of these discussions that we're having in this group are still impaired by the fact that we don't have final solutions on the data protection agreement that were an outstanding action item from Phase 1 of the EPDP.

My question to you is what the plans are and whether there's a potential delivery date for the data protection agreement between

---

contracted parties and ICANN and [your] position from Phase 1 because we're basically building on that. The concepts that we're working on depends on the outcome of that.

GÖRAN MARBY:

Yes, the courts have the final say, but our intention now – I don't know about you, but I will tend to trust more the recommendations if we get some from the European data protection authorities more than at least my own legal opinions. As you know very well, the guidance from the DPAs has a legal status, which is that's where we're going.

The problem I think is a little bit of a Catch-22 right now. We are testing a legal model for trying to do this, and we don't know the answers to some of those questions that we posted. I agree with you: documentation is a very essential part of the relationship we are having. Also, you have to do it according to a law. But we also need to figure out the actual model to be able to sit down and do all those papers.

So I think that we're in a Catch-22 situation because you have to assume – if you agree with me 100%, then you think that this is the only-way model – yes, we can do it – but I don't agree with [inaudible] because I think there's a potential we're not going to end up there. So it's hard right now to do all the scenarios for the different versions of doing it. So we take the assumptions that the legal responsibility for the contracted parties who are making the decision will stay with the contracted parties.

---

Let's make the assumption that you come up with a standardized format for that, for asking those questions, and the contracted parties agree that you will [answer] in three days or two days or 12 minutes or whatever it is and we're all going to ask questions. That doesn't change the legal standing. So that could [fit]. But with the model as itself right now we don't know the answer.

So I agree with you. It should be documented. It should be a lot of work. But we don't have the answers right now. But hopefully we will get the answers. When Elena and her team we start asking questions, your first question would be, "How long will it take? What is our time plan?" But I would leave that over to them to talk about that because we are not talking about eons of time anymore.

JANIS KARKLINS: [Briefly].

THOMAS RICKERT: That's great, Goran. I agree that we still need to answer a couple of questions. I think it's in our control though to find a way to mitigate some of the risks [inaudible]. I know that this might not be popular for everybody in the room, but I guess that the joint controller scenario – I'm publicly committing to a joint controller scenario – would mitigate the risks to the best possible extent for me. If, let's say, the registries, registrars, and ICANN determine that they're independent controllers or that they have a process/controller relationship and actually a court determines at some point that it's a joint controller scenario, then you might be

---

sanctioned for not having put in place the appropriate agreement. But, if there's a controller process, I'm going to still say that you're a joint controller. So that's a safer route to take.

I guess the mere fact that Trang has recently resubmitted to the list a link to ICANN's record of processing activities and that document is missing one of the points mentioned in the law – i.e., naming who's the controller for the processing [inaudible]. So we still don't have certainty on that. I think we could advance these discussions by having the contracted parties in ICANN work on such agreement. Then you can allocate functional responsibilities in such agreements where you make certain parties inside those constructs [inaudible] certain types of processing. I guess that's what would help everybody to be able to inform the data subjects about how the data is being processed and fulfill the information [activities], Article 12 to 14, which nobody in the industry can do at the moment. I guess it would also help us in building on the outcome of the first phase of our work.

I can elaborate more, but I don't want to spend too much time on this.

GÖRAN MARBY:

There was a couple of things that you say. This is far beyond [me]. You're much better lawyer than I am. Let's pick a couple points. The risk. First of all, we don't determine who becomes a joint controller. As you said, somewhere down the road, either the DPAs give us advice or it ends up in court because you and I can declare ourselves to be controllers and we can act as we were. But it doesn't mean that it actually happens. Even if we write it

down, it doesn't mean that it happens because it's not up to us to make that decision. We can act as we were, but in the end, the court or the DPA would decide if we are. Otherwise, it would be very hard with law. It's actually [inaudible] and I think most people know that. We can say we are, we can act as we were, but in the end, we don't know. So there'll always be a risk. And you said you agreed with me [inaudible].

The other thing is the concept of joint. Joint means joined by the hip. Joined is not really fairly defined in the sense because who has responsibilities? So joint means that you actually have a shared responsibility. I'm just taking an example now. Let's say that we have some of the data for something and we have a data breach. What is your legal responsibility in a joint relationship for that data breach? Now you will say, "Oh, we put that in the contract." But we will not know that until someone said that we now accepted it because joint means joint.

I'm asking myself, is a company – then how big are ... Let's say we now establish that joint means joint. But if we do a mistake, you're responsible for that mistake. How much do you actually pay for that? If you Google, or anyone else [inaudible] because we would of course never have a data breach or anything because we don't have the data. But [let's lead] with the example. Does that mean that Google will have to pay 4% of their turnover for that [inaudible]? You and I will say – which I will not disagree with you. We fixed that with the problem. The problem is, until we actually know more about it, how do we know that's the case? Because it's actually [not defined].

---

---

So I agree with you. It should be documented. It has to be. There's no question about it. It's just that I'm not and we are not there yet. We want to figure out some more things because we take that step. I agree with anyone [inaudible]. We can't wait. But we can't put the cart before the horse. Is that an expression? Thank you. I seem to invent my own expressions sometimes. It is? My new favorite is that every silver lining is attached to a very big, gray cloud. That's my new favorite [after this]. It's very hard to put an elephant [in a mini]. That's another one I came up with this week.

But you see. So we have no intention of doing anything else in trying to solve this problem, but we're trying to the fundamentals before we go down this road. And I think that's where we are. So no disagreement about what's going to happen when we actually have some more information [about this].

JANIS KARKLINS:

I think time is ticking. We have three remaining flags up. I will take those three before we go to the next topic. It will be Stephanie, Milton, and Brian.

STEPHANIE PERRIN:

I'm going to make this remark personally except to say that, as head of NCSG, I'm always saying we're here to help. If you need a lawsuit, I offer. Just talk to me. Because it does seem to be we're going in circles here. We need a lawsuit. We can't have a decent lawsuit until you decide whether you're a controller or not, really.

GÖRAN MARBY: We can. You can just go to the DPAs.

STEPHANIE PERRIN: Well, sure, we could. But we need some facts and we've been chasing our tails for the last three years on this, as far as I am concerned.

You mentioned a while ago that it would be easier if ICANN had a privacy policy. It seems to me we have to be clear here. ICANN has to have a privacy policy if it's going to take on any responsibility in terms of the disclosure instrument because you cannot just sweep the determinations that you're going to make on these balancing tests under the rug of public interest or any other broad bylaw statement on the part of ICANN. These are not the kind of privacy policies that one had 20 years ago. They've got to be specific in terms of the data.

I'd just like to remind everyone, but particularly Alan because it is attractive to think that ICANN is a controller and the contracted parties are mere processes, that most of the money that they make from the individual is from other services. So they have a relationship with the individual that goes far beyond the data that shows up in the WHOIS, and anybody that's got a serious criminal investigation is going to go for the financial data, the IP address and any other data in the network that is interesting from that perspective, which is far beyond what we're talking about here. I wish we could just kill that one, you know, and make some decisions here about these agreements because we could debate

---

them until the cows come home and we'll never have a court case if we continue. Thanks.

GÖRAN MARBY: So the cows come home? Now we're getting there.

STEPHANIE PERRIN: Or I could also say this train has left the station. How about that?

GÖRAN MARBY: So the remark is really about we are very much talking about the European Data Protection. There will be other ones, a nuance. And if we try to manage our policies according to all, I mean basically I believe it's all going to be the same underlying perspective of them, but they're also going to be slightly different. So the underlying principles how we do things hopefully that could be whatever you come up with, those underlying principles should be more than just a European law. Of course the European law is the best one ever and etc., etc. and a role model for the rest of the world. But we will see other – I mean here in California, there's something happening. India is doing something. So that's what I mean. It's hard.

Making a policy is very much based on one particular [situation], but it's one particular legislation. Yes, it's for 27.5 member states but it's still covering a fairly small part of the world. So that's why I personally in a personal capacity think it's good to have sort of policy for privacy. WHOIS is not the only source and not the only database we have. It's a database we don't have, to be honest.



MILTON MUELLER: I want to follow up on your interaction with Chris Lewis-Evans. He was making it clear to you that our process – I don't necessarily say ICANN but certainly our policy and ICANN in terms of implementation – will have to accredit the accreditors, and you kind of ducked that in my opinion and said that GAC could do something about that. I'm looking at GAC and I don't think they're going to do anything – they're not going to burst a treaty that gets you out of that obligation.

Again, we've discussed this aspect of accreditation today and it's pretty clear that whoever is accredited to make the kind of decisions that you want them to make, there's going to have to be accountability, there's going to have to be transparency, there's going to have to be auditing of how that ability is used, and where is that going to come from if not from ICANN and its policy process?

GÖRAN MARBY: I really don't understand the concept of question. It's because what I'm trying to do is to give the ICANN community for its policy-making process that. And I pointed the other side of the table here. Here is its people that actually have to make the determination of access to the data by the law. So in your scenario, if they don't accept that someone else is doing this, we can legally prove that.

MILTON MUELLER: Probably that's your scenario, not my scenario.

---

GÖRAN MARBY: Oh how? I ask you guys, would you let someone else take a decision about increased liability to you guys?

MILTON MUELLER: I don't understand how you're responding my question. Do you accept or not? The fact that we can't just magically wave a magic wand and have INTERPOL and WIPO making decisions about who is accredited without following it up, without having a policy regarding who is accredited and who is not. That's my point.

GÖRAN MARBY: I don't think I've said that, Milton. I don't think I've said that.

MILTON MUELLER: It sounded like that's what Becky would say.

GÖRAN MARBY: That's not what Becky was saying.

MILTON MUELLER: Becky was saying, you go to a [condiment], you get accredited, and once you're accredited, all you do is interact with the system to verify that accreditation and you get the data.

---

GÖRAN MARBY: Did she say we're not going to be transparent, control it, all of that? Have you looked at [COC] model?

MILTON MUELLER: Never mind. This is not being a productive conversation.

GÖRAN MARBY: Milton, I have no problem that we disagree on some of the assumptions. I have no problem with that. I agree with the fact this is not a simple doing. But it's hard for me when you say something that I'm not trying to say and I'm trying to really drill down to make sure that at least for the rest of the audience, I'm trying to say what we believe in. You might not agree with me, and I'm totally fine with that. But we also say in the end of this, Milton, is that the result of the questions will be going out of this process, which is my job is to provide to the policy-making process – that's you guys – to make whatever you want with it. I'm not making this decision in the end. You are going to make this decision. And if you don't believe that the system is itself – if you don't believe that we will be able to do this, I'm fine with that because we don't know if we actually knew, it wouldn't have [inaudible] process we're doing. That's why I'm liaising the process.

JANIS KARKLINS: Thank you. The last is Brian.

---

BRIAN KING:

Thank you. I thought Milton was going to go where I was going to go, coming out of the conversation with Chris. To be clear, I don't think that anybody was on the wrong side of the line here but I would caution this group in general to be mindful that we should develop a policy ourselves and we need to make this work as an EPDP Team. While I think our lives might be easier if we did have some clarity from the Data Protection Board or the European Commission about ICANN acting in the public interest, that's on ICANN to do. That's for us to do as a team. We were on a post-IANA transition world and the IPC is committed to multistakeholder model like everybody else in this room is. We're not of the behest of one government to approve our activities here. So I just wanted to be clear about that. Thank you.

GÖRAN MARBY:

We do agree on the fact but I think – we can't just name ourselves an accreditation house according to the law. Someone has to call us that. And that has been done by the decision by our government. Probably in Europe, there has to be 28 governments. It could be one. We don't know. But someone has to name us that. We cannot decide that in ourselves. That's not a bug in the law. That's a feature in the law. Are we done?

JANIS KARKLINS:

I think so, at least for the moment. I think that we will be done only when Board will approve the policy after Council will approve the policy, so then we will be done. And I hope that that may be in March. That is my objective. That's why you need those not to

---

hurry up but to keep our calendar in mind. At least we're working towards that objective.

What would be my observation and conclusion from this conversation? First of all, thank you very much for interacting with us and I think we need to continue this dialogue on every occasion, then we're in the same place in the face-to-face and if need be, if you have something to share with us, we would be glad to receive whatever information you could feed from interaction with the European DPAs and any confirmation or dismissal of proposal.

From other side, I'm looking to what you're planning to do. I would suggest think also on less of these cases for the non law enforcement and the Intellectual Property group. There might be some difficulties in that determination who will be the body who may provide accreditation and clarity or even given the decision whether data should be disclosed or not. Using just simple examples may mislead us from the final goal because we need to look on every possible case.

So, we are determined to continue and we will now maybe go to our Strawberry Team representatives here to hear what is coming up and then what kind of information we can get from them. Thank you, Goran.

GÖRAN MARBY:

Thank you. I'm just going to check with – did I miss anything essential today? Anything you need to correct, by the way? Thank you very much for having the opportunity to talk to you. I was

---

trying to be as fair as I can. I tried to be as transparent as I can. I promise you, if there's anything happening to this, I will let you know. As nice you were to me, to my team who represents the Strawberry. I told them if you come up with a better project, we are open for suggestions.

JANIS KARKLINS:

Welcome, Elena and the team. Probably I will do exactly the same thing that I did with Goran. I will simply invite you to try to answer the questions that we submitted prior to this meeting, what is the expected timeline in which Strawberry Team plans to engage with DPAs, and have you had meetings with DPAs after the Marrakech meeting? If so, is there anything you want them you can disclose for the purpose of our activities. Elena, please.

ELENA PLEXIDA:

Thank you, Janis. Thank you for having us here today. Good to see you again. I'll go straight to the questions, starting with Question 1. Bear with me a little bit because I want to give a little more information than just give you a date, which is when we expect to have the Board answering back to us.

So allow me to start by saying the UAM is one of the [possible] ways to implement SSAD. It's one side of SSAD. It's implementing SSAD in a unified fashion. It is based with a very simple notion that to have a uniform, centralized way for dealing with disclosure you have to have a centralized system, the parties assumed with must not be responsible for what the center is doing. Otherwise, they would not want to participate in this. It's as simple as that.

So with what we call the UAM, we are creating a system where contracted parties do not imply their individual judgment who gets access to what under what circumstances, etc. Assuming [inaudible] means that if they don't have responsibility on the disclosure and therefore they don't have the ability.

So what we're doing now is we're taking different assumptions. I'm repeating that just to reiterate that's all that the Strawberry are intending to do right now with the DPA is just to check whether this assumption is true. In that spirit, at the moment we are contemplating three questions to ask the DPA which are more or less the following.

First one is [taking back] to the space. It will be asked more or less with this proposed UAM centralized responsibility for disclosure or in other words, consolidate responsibility around disclosure in the system and hence remove this responsibility from the contracted party.

The second question is a follow-up to the first question. We want to ask whether there are any other steps that we haven't thought about as a matter of politics to ensure that this system will take full responsibility for the disclosure activity of [inaudible].

The third question has to do with the way the system is designed. So as a reminder, the CSG has designed the system whereby the central gateway is obtaining the full registration data, just filtering it, and then takes it back to the requestor. As opposed to let's say only obtaining the fields that are relevant data request and maybe send it back to the requestor, not to the gateway. Right? Again, this is designed in the assumption that that way, the contracted

---

parties who have nothing to do with the judgments and they have no way of figuring out who was the requestor or what was the request about.

So the third question wants to ask based on this design and on the idea that the contracted party doesn't have anything to do with the judgment. Is that acceptable? Because there's a data minimization principle in GDPR which would say, "Why don't you send directly the data to the requestor?" Besides that, there are also cases of operational secrecy that's need to be obtained for law enforcement, for example.

These are the three questions we are thinking about. Again, I repeat, we are only trying to see whether by having a sole party with access to nonpublic data is possible, whether we can consolidate the responsibility around disclosure. So in whatever form we introduce these questions to the DPAs, we will make sure to also acknowledge that there are other legal issues that need to be looked into such as the International Data Centers which is an issue. And maybe we will look at in the future the other matters of developing appropriate safeguards for the data subject, or as Stephanie was explaining, for the accreditors and [inaudible] and all these things. But there will be a disclaimer saying that we understand all that, that these are to be developed further on by the policy [inaudible]. And of course we will repeat to them what we have already said that it is not ICANN Org that designs any model. The model is to be designed as well as the policy around it, it should be designed by the community. Therefore, this is intended for the work of the committee which is already ongoing.

---



With respect to timeline, next week we are meeting with European Commission and all activities with the European Commission which are confident [inaudible] of the European Commission to formulate these questions. The Commission so far has given good advice. I pointed out before we need to make sure we formulate them in the right way when you talk to the authorities that are responsible for data policy [inaudible].

Apart from discussing with the European Commission about how to formulate the questions as such, we're going [inaudible] what is the best and the most appropriate way to introduce the questions to the DPAs, which is also important issue.

Once we're done with the questions, the drafting is okay, we are able to forward them to the DPA. Now, to get an answer from the DPA, we need the plenary of the Board. The next plenary is actually happening tomorrow and the day after tomorrow, so forget about that.

The next one is 8 and 9 October. And the one after is 12 and 13 of November. Now, we need to keep into consideration, into mind that before our questions, the ICANN questions go to the plenary, they have to be looked at by what is called the Technology Subgroup. They have a subgroup that actually looks into it and recommends to the plenary what they should come back to with us. These groups they usually come together a couple of weeks before the plenary. So I'm saying that to say that I'm not sure that we can keep the 8 and 9 October plenary. But I'm pretty sure we will keep the 12 and 13 November plenary following which we can [hope for another].

---

---

We will update you after the meeting with the Commission next week or you can hear directly from the Commission on that. With your permission, we're also hoping to liaise with your liaisons following that meeting and following your face-to-face to make sure that whatever we have put in the questions, whatever we send to the [dedicated team] is not by any chance contradicting what you have decided in your face-to-face meeting with respect to the zero draft, particularly the policy that's put in place with this.

JANIS KARKLINS: The second question is about interaction with DPAs after Marrakech.

ELENA PLEXIDA: The quick answer is no, I mean in the sense we didn't have any formal meeting with them and discussion with issues, not at all. But if you're asking generally if we met them, I met with the head of the new Belgium DPA exchange in a cocktail event in Brussels during the summer. Well, I felt like I need to [inaudible].

JANIS KARKLINS: Thank you, Elena. So now we have a few flags up. We'll start with Ashley, Alan, Alan, Alex, and Thomas.

ASHLEY HEINEMAN: Thanks. This is Ashley with the GAC. First of all, thank you very much for this update. I think that the questions sound like are right in line with the information that we need to get back. I also

---

appreciate the fact that you're doing this in a way that kind of recognizes and respects what's happening in this group. The intention here isn't to guide our work necessarily but to inform it.

With respect to timing – and I don't know if I should be looking at you or Georgios Tselentis, but I'm really concerned about the timing. We are running out of time at least with respect to the constituents I have to respond to back home. This is I think really important that we have as much input into our report as possible going into Montreal, and it sounds like based on the timeline here that that won't be possible.

I understand it's difficult to deal with schedules of other entities, but if there's any way that we can meet the October timeframe, I would urge you to do so because I think, one, besides me not wanting to get my head chopped off back home, I really would like – I mean this is information I think is really critical to decide in the path that we take. So I'll leave it at that. Thank you.

ELENA PLEXIDA:

This point taken and we'll try to do that. I don't know if Georgios wants to add something. My only point would be indeed it's difficult with them and I wouldn't feel okay with rushing them into something they don't understand. Georgios knows better.

GEORGIOS TSELENTIS:

There's one thing to get a formal – because what Elena described was the formal procedure to get something from the Board, written questions. I don't think – I'm not optimistic it has something else. So I think it is as Elena is describing, if you are looking for a letter

---

coming from the Board then it has to go through the procedure that she said. I don't know if we can make some sort of informed decision based on informal interaction and this I have to ask my colleagues how we can base this in our discussion. But the formal I think is – the timing is what Elena is [inaudible].

JANIS KARKLINS: Thank you. Now it's Alan G.

ALAN GREENBERG: Mine is very short. Georgios may have just answered the question. I'm not sure. If you make the November meeting, when can we expect a written answer? Is it at the end of that meeting or is it seven weeks later or what?

ELENA PLEXIDA: I can take that. Based on previous experience, because it is the subgroup that has actually prepared the answer, a few days after the plenary, shortly after the plenary, we should expect that.

JANIS KARKLINS: Thank you. Alan?

ALAN WOODS: This is more kind of a personal worry. Again, in talking to Goran as you were hearing, based on things that Thomas is saying, I just have a worry that again one of the issues with going so closely to the DPAs, this particular moment is that our houses are not in

---

order. It's as simple as that. They are not in order and we continue to jump up and down, waving our hands saying, "Hey, look at us," because we're over here without a protection agreement in place.

I mean I can only urge caution. It's like we don't want to attract too much attention after that as well because it would be a huge issue. And if we're talking about security and stability, every single registry and registrar out there getting fined straight away as a [uni] would be slightly damaging to the very core of the Internet I would think at this particular moment in time. But again, it's just a personal worry that I have that we are trundling forward into a very dodgy arena and we're not ready for it yet. But that's all I'll say.

JANIS KARKLINS: Thank you. Alex is next.

ALEX DEACON: Just two quick comments and then a question. One is could you provide the questions you're going to ask the DPAs in writing to us just so we see them? I was trying to take notes as you were describing the questions but I want to make sure when I report back to my clients and constituents that I have it accurate exactly what you're going to be asking. If you could do that, that would be great.

I'm also concerned about the timing. I think you should try really hard to get those answers by the October meeting if possible.

---

The question again is, I was looking at your presentation from Marrakech, July 27<sup>th</sup> presentation where you described the engagement with European DPAs to date. The last engagement that you stated was 13 July 2018. I know you've had this cocktail and I appreciate that. That was 11 months. Since then, other than the cocktail, there have been no other formal meetings with the DPAs. Is that correct? Okay. Thank you.

JANIS KARKLINS: Thank you, Alex. Thomas, next.

THOMAS RICKERT: Thanks very much. It's basically adding to what Alex has asked. Is there any written material that you previously provided to the DPAs describing the concept exactly how you envisage it? For them to have a basis for asserting your question, because I find it quite abstract or difficult to imagine because our group is not able to grasp what the setup with such concept could be. So I was entirely puzzled as the Data Protection Authority is set to answer a question and you seem to be able to do that. That's a material that can also help us.

ELENA PLEXIDA: The questions are related with those. We do have the working just as we are working on a [inaudible] introduced these questions. We will explain what the model look like and what the question is, what the problem we're trying to address. As I said, we will update you after the meeting with the European Commission where we hope to have a better draft with input of European Commission

---

which is invaluable for this particular exercise. We will share with you after meeting with the European Commission including the questions.

JANIS KARKLINS: That's in two weeks' time.

ELENA PLEXIDA: Yes. Next, next week.

JANIS KARKLINS: Thank you. It's now Marc and James. Then Ashley.

MARC ANDERSON: Elena, thanks for coming and speaking with us. Again, we appreciate the update. A couple of my questions were asked already, so just leaving me one to ask. Actually, you have been following along our work. I know you mentioned the SSAD model. I'm curious, the work you're doing and the work we're doing, are there any thoughts you have on what's going on in our group? Do you have questions for us? Have you looked at the zero draft? I'll maybe pause there and let you just –

ELENA PLEXIDA: What are you doing tonight? We're also liaising with Trang and Dan who are with you all the time to get things – we don't [inaudible] straight. As I said before, we particularly want to wait for a few face-to-face meeting to be sure that whatever you have

---

agreed is aligned with – I believe it would, anyway. We particularly want to wait for these face-to-face meetings to be sure that whatever you have agreed is aligned, which I believe it would anyway.

MARC ANDERSON: Thank you. You certainly got to the heart of where I was going with that. Or are you finding we're doing things that are out of alignment or are we in alignment with the work you're trying to do?

JANIS KARKLINS: James, please.

JAMES BLADEL: Just briefly. I wanted to take a slightly different tack than my colleague, Alan on giving the DPAs the visibility into our industry when our house is not in order. I don't think at this stage of the game anyone really has a completely clean house ready to entertain guests. I think that the risks of not asking these questions outweigh the risks potentially of drawing attention to us. In fact, I think one possible outcome of drawing attention to us would be that they come down with a whole bunch of remediation and/or pure instructions, which hey, that's kind of what we're looking for anyway.

So I feel like we shouldn't be bashful is where I'm going with this. I don't mean to be dismissive of Alan's concerns, but I also think that now is not the time to hold our tongue because we might not get another opportunity when the rest of the world and other



---

industries have gotten their houses in order and we're still struggling with these things and wrapped around the axle on these questions. So I would encourage you to ask away, be as honest and forthright as possible, don't withhold anything you feel might be material because I don't think we're going to get another chance like this.

JANIS KARKLINS: Thank you. Ashley?

ASHLEY HEINEMAN: Thanks. I wholeheartedly agree with James. I'm sympathetic to where you're coming from, Alan. I supported – since in the past we deferred which is what we have done. But I think at this point in time, really time is of the essence, and if we have a luxury of having European Commission at the table to exist and making sure we're asking the questions in a right way, but I just find that we spend quite a bit of time on this chicken-and-egg thing so we couldn't get some answers. Even if they're not answers that some of us like, I think just getting answers to this point is actually critical.

JANIS KARKLINS: Thank you. I think you're getting lots of guidance. I think it was Stephanie – sorry. Milton, Margie, Stephanie, and Alan.

---

MILTON MUELLER: I don't know if you're familiar with the background history here but ICANN has a long history particularly on this issue of the organization deciding what they want the policy to be and the multistakeholder policy development group being kind of window dressing. Then at the endgame, there's a horrible clash of expectations in which the policy process recommends one thing and ICANN Legal suddenly says, "No, we can't do that." So I'm actually a bit confused by the mere existence of your committee. I know you're not responsible for it. I don't want to really go after you, but it's like why is your team interacting with the DPAs rather than interacting with us more regularly? We could have fed you questions we wanted answered many months ago. You say things that make us very nervous like, "We are creating a system." Sure you don't mean that but those words just keep coming out and what you mean is – as Becky explained to me once – you are hypothesizing that if the system is created, what would be the legalities or something like the responsibilities and so on. But is there any way for you to view what you're doing as a part of our process rather than a parallel process that threatens to marginalize or conflict with what we're doing?

ELENA PLEXIDA: First of all, I'm not a native speaker and I use this as an excuse as often as I can. And it's actually true. So yes, what I said we are creating, I meant [inaudible]. We're not creating anything. We're just having some ideas. Then as you know, Strawberry will cease to exist the moment we get the answer from the DPAs, which comes back to you for you to do whatever you want with it. So I

---

think this stops any parallel whatever exists or it is used as it is right now.

I would like to reiterate what Goran had said I think several times. If you have any questions of any sort that you think that needs to be answered by the DPAs, we can channel to the Commission [inaudible].

JANIS KARKLINS: Thank you. The next is Alan G., Margie, Stephanie, and Thomas. No, no Thomas. I would then want to draw the line.

ALAN GREENBERG: I just wanted to support what James said and supported by Ashley. There's always been a perception amongst some of us that the DPAs thought WHOIS was a lot simpler than it really is and thought it was just a big database that we had sitting over on the corner of the floor. And anything you do at this point to educate them and to just how complex these things are and by looking at the solutions, I think you're doing that clearly. I think it's a good thing. We can't keep on going the way we are right now, so I strongly support what we're doing.

JANIS KARKLINS: Thank you. Margie is next, then Stephanie.

MARGIE MILAM: Sure. I think I echo the comments to Alan, James, and Ashley. But one of the things that Milton raised I think something we need to

think about, to the extent that we know that we're going to get answers on certain things, if the answer is that it's possible and it does alleviate the risks the way that you [search], it almost seems like what do we do as a group? Do we wait to develop some parts of the system until we get that answer or do we end up in a situation where we have a policy that actually is going a completely different direction? Like Milton said, we may end up in a different place because we don't have the answers. So we might end up in a more conservative system because we have this big gray area on the liability issue.

So I guess that's my question to the group. Do we reshuffle the way we do our work so that we don't have the situation that Milton has described that we come up with a policy that isn't remotely close to what is possible if we get the right answer from the DPAs? That's my question to the group.

JANIS KARKLINS:

Look, Margie, I think we will talk about this, how to interpret what we heard in the past two hours and how to factor that in our activities. I think our task is very large and elements that we need to address are somehow linked that they also could be addressed in parallel, and most likely we need to continue working on every issue in parallel and then at one point see how we could factor whatever answer comes in from the DPAs in our model that we're working on. Stephanie, please.

---

STEPHANIE PERRIN: Thanks very much. Like Milton, I understand that you're operating under a set of instructions and assumptions here. But I'm a little concerned that this group has not decided that we can afford such an access model or that it would be acceptable from a policy perspective, and yet we're consulting the DPAs on how to build it, which is an implementation issue. Hopefully along privacy by design grounds, the principles, but we haven't got the policy yet.

So while I understand the urgency and we have been circling the drain for three years at least, if not six, depending on where you start counting – 20 in some cases – they told us in 2003 that we could build a layered access model. They know that. It's all over the Berlin group report that they tabled a couple of years ago and many of the guys that are on your Technical group are also on the Berlin group. So I would also argue that if DPAs don't understand this problem thoroughly, it's because we haven't explained it to them. So, for instance, nobody explained the [inaudible] transition concept to them. But they're not completely oblivious the knowledge of this stuff. The Assistant EDPS (European Data Protection Supervisor), the polished gentleman whose name I can't pronounce has worked in this area, so he understands it pretty well and he came to a panel, we did a RightsCon and discussed some of the finer points. So let's not assume they don't know about this and aren't waiting for us to follow the logical step which starts with a privacy impact assessment so we know the risks that we're trying to alleviate. Thanks. Sorry to be a broken record on this but we've got to start at the right end of things.

---

JANIS KARKLINS: Thank you, Stephanie, for your comment. So no more questions? Do you want to conclude something, say something at the end?

ELENA PLEXIDA: Thank you. We'll update you as I said after the meeting with the Commission. On my side, I'm not an old-timer in ICANN. I'm kind of an old-timer on things [inaudible]. The only thing I would say that it is in the European mentality that when you engage, you really saw that you are trying to solve the issues, so of course we're not going to say, "Here are our problems." But in the European mentality, the more you engage, the more you show you're ... it's actually not something bad but it's actually [inaudible].

JANIS KARKLINS: Yes, Thomas.

THOMAS RICKERT: Just briefly. Elena, can you just verify for us? Alex and I wanted to – were you saying that we will receive any brief document or the questions only after the meeting with them?

ELENA PLEXIDA: After the meeting with the European Commission. Of course before the meeting or whatever it's going to be, forward the questions to the DPA.

---

THOMAS RICKERT: Is there any chance we can see before that? Because I guess that was the purpose of the question that we can check whether that's potentially contravening the interest of this group.

ELENA PLEXIDA: Thomas, [inaudible]. It's a working [inaudible] but we can't be sure right now. Personally I don't feel confident with the way it's written right now, to be honest.

THOMAS RICKERT: Just for the record, so you're confident to share it with the authorities but you're not confident to share it with us?

ELENA PLEXIDA: No. By the time the meeting is going to take place with the European Commission, it's not going to be the working [inaudible] that it is today.

ALAN GREENBERG: With the European Commission, not the DPAs?

JANIS KARKLINS: I understand that based on whatever outcome, we will produce or understandings we will reach by Wednesday. The questions may be modified or at least ... yeah, may be modified. Now since this meeting was recorded and the record will be available a few minutes after the adjournment of the meeting, so you can listen to the recording and capture what Elena said in this meeting. So you

---

will have the questions as they were explained to us during the meeting.

So, thank you, Elena. We're looking forward to receiving all information you can share with us and thank you for factoring in whatever we do here and on whatever stage we are in our reflection in the policy development process. Thank you very much.

With this, we have been in session a little bit more than two hours and I feel that it's better to break now and come back after 15 minutes and then discuss what lessons we can draw from interaction with Goran and with Strawberry Team with Elena before continuing with our conversation on accreditation issue. Now it is 3:20, we reconvene at 3:35 and we will start with sharing impressions from the conversation. Thank you.

Welcome back. I see that the discussion with Goran and Elena energized the team. For this segment, my intention is simply to collect maybe impressions that you may wish to share with the team from the conversation with Goran and Elena and particularly how you see whatever you heard and understood with impact in any way our plans for our work and way forward. That's the question that I would like to ask and if you can share your opinion in a brief fashion. Please, Alan.

ALAN WOODS:

Thank you. I suppose two of the main takeaways from that I saw – and again we have to take it with the intention that it was, that it wasn't exactly a solid statement or not from Goran – but there



---

seems to be a feeling that they do not wish to end up as the sole body who is going to take any additional indemnity or to be the person who is this accreditation body. So I think we need to be able to when we're going through this, yes, obviously the policy will be led by what we decide but the level of which it will be bit of pushback, I can assume that we should prioritize them lower down in our pecking order just based on what we heard today.

JANIS KARKLINS: Thank you. Brian?

BRIAN KING: Sure, thanks, Janis. Probably a couple of takeaways. The first that comes to mind is that I was encouraged that Becky seems to be on board. I don't know. She probably didn't try to speak for the whole Board or the Board's opinion but it seemed that she was on board with accreditation and that kind of hamburger concept could work. So the requester could go accreditation body and that could facilitate entry into that. So I was encouraged by that.

JANIS KARKLINS: Anyone else? Milton? Sorry, Ashley first then Milton.

ASHLEY HEINEMAN: Thanks. Ashley with the GAC. Just to maybe disagree slightly with Alan, I heard a lot of non-committal responses and I took that not necessarily that they didn't want to do it but more of we want to hear what the response when we get back from the DPA is our

---

first. So we wouldn't want to lower in priority the hamburger model because we got non-committal responses.

JANIS KARKLINS: Okay. Milton?

MILTON MUELLER: Well, I was kind of discouraged by the same things that Brian was encouraged by, which is that clearly they've decided they're still calling it the UAM. They want to have a UAM even though we haven't made a policy decision to have one. But they have decided what accreditation will look like even though they tell us that we'll decide that. It's pretty clear they've worked that out and they have a very specific motion in mind which Becky elaborated on at length. Where she got this idea, I don't know because it certainly wasn't from us.

I agree with Alan that when you try to pin them down on what exactly role ICANN would play, we get this horrible "I didn't say that" then we get into these misunderstandings that it seems to happen every time I try to engage in a public and exchange with Goran. So I think, to me, this really has almost no impact on our policy development. We continue what we're doing. We are the legitimate policymaker. There's nothing they said that would rule out any of the options that we've been discussing. There's nothing they said about liability or the distribution of liability, a concept which he ambiguously tried to deny existed. There's nothing they said about that that would alter any issues that I can think of in terms of our approach.

JANIS KARKLINS: Okay. Thank you. Alan G.?

ALAN GREENBERG: Caught in the middle of a popcorn. I guess I'm still a little bit worried about the amount of hand waving. One of the easy cases that everyone seems to be talking about is Europol as is the INTERPOL. And yet, that's one that's just isn't going to work. INTERPOL treats all police forces around the world as equal, anyone who are members. For China it's equivalent to the U.S. If you're going to use a contract party, you're going to release information based on a police force need. It can't be done universally without regard to where the request is coming from. So those kind of decisions are going to have to be made based on where you are and who your police people trust and it will not be an INTERPOL accreditation that's going to work. When the simplest one is really one that won't fly at all, I worry a little bit. The only encouraging part is they're working with the European Commission and that gives me some confidence the European Commission thinks of whatever we're proposing might fly.

JANIS KARKLINS: Okay. Thank you. Hadia?

HADIA ELMINIAWI: I tend to disagree with Milton. I actually see that what we heard today does really inform our way forward. The problem is that we don't have the answers yet. However, one important thing that

---

was mentioned today that the aim of having a unified access model and the questions actually drafted that are going to be drafted by the Strawberry Team, they ask directly or are related directly to reducing the risk associated with the contracted party. Especially in relation to who makes the decision-making and who makes the determination and if this would actually reduce the risk associated with the contracted party. So actually, if we have answers to these questions and we realize that there could be an effect on reducing the liability of the contracted parties that maybe we would actually choose a different way than if we don't have an answer. I was happy with the conversation today. The only thing is that the answers are coming in maybe a little bit too late.

JANIS KARKLINS: Thank you. Matthew?

MATTHEW CROSSMAN: I just want to pick up on the conversation that Alan and Ashley were having. I don't think we disagree, but I do want to clarify one thing that I think Goran was pretty clear that they're not willing to indemnify contracted parties. I think we all heard that. I think that's actually helpful, help to kind of focus our discussion on liability. It doesn't rule out liability shifting necessarily but we can take that off the table and focus our discussions going forward.

JANIS KARKLINS: Okay. Stephanie? Stephanie, please.

---

STEPHANIE PERRIN: I don't want to sound like a broken record. And I really appreciate the work that staff is doing and how much support they give us. Don't misinterpret this. I'm deeply concerned about staff being under instructions from somebody other than this working group that is working – their collective [inaudible] to come up with a policy and they're figuring out the questions, not informed by our policy discussion. I understand that this is Goran's baby and he asked the Technical Study Group to go ahead and see if this could be done. I said, "Okay, fine. That's an RDAP demonstration." But this is going further and further down the policy road, and I tried to express that politely but really, we might as well all go home if all of the important decisions have already been made. Because I don't want to waste my life spending – it's already been six years here of not being listened to. We drag the late Giovanni Buttarelli here to try to inform people – may he rest in peace – of what the roles really were. I don't think that was ever properly followed up. It's pretty discouraging. There's gestalt here that we're going to go ahead and build another WHOIS, and I don't see that changing. So if that's going ahead and figuring out the questions that should [be] asked the DPAs for a model we haven't agreed to be built, why am I here? Why not just leave?

JANIS KARKLINS: Stephanie, I can tell you that staff supporting our work is not influenced by anything that goes outside this room.

STEPHANIE PERRIN: I understand that. I understand that and that's why I tried to –

JANIS KARKLINS: We need to be absolutely assured by that. So marching orders supporting staff of EPDP Team gets from EPDP Team also from me and from no one else. So that I tell you with a full authority. We need really to stick with that and not question at all.

Brian and then Marc.

BRIAN KING: Thanks, Janis. One other opportunity that I think we uncovered today is the opportunity to be clear about which processing activities we're talking about. We talk about liability and we talk about when that happens or what that means. Even within an SSAD there's going to be different processing activities and one's going to be the disclosure of decision-making and another might be the actual technical disclosure of the data. And there are others that probably we haven't talked much about like storage of the data, perhaps encryption, and some of those other processing activities. And as we're thinking about liability and where that lies and how that's structured, I think it will be helpful if we're very deliberate about the processing activities that we're talking about first, and then liability for those. Thanks.

JANIS KARKLINS: Thank you. Marc followed by Thomas.

---

MARC ANDERSON: Thank you, Janis. Coming out of the meetings, I was struck by how many certified foundational type answers we don't have yet. Probably all of us were hoping we'd have more answers by now. We had the TSG model. I think it was finalized in Kobe. We first heard from the Strawberry Team in Marrakech. And Thomas pressed Elena on if we could see the questions. She was not prepared to share them with us. I think that was disappointing to me at least.

When we're talking about this, we come in to this meeting with Goran and the Strawberry Team, we knew we might get answers, we might not get answers. But either way, we know something. So our job now is to react what we heard or didn't hear and figure out, okay, based on this, how do we go forward? We know we might get answers from the Strawberry Team at some point in the next few months. But I think we have to figure out how to go forward how to start making these decisions ourselves. Some of the foundational questions like decentralized versus centralized. We're going to have to roll up our sleeves and start tackling them ourselves. Get in to the nuts and bolts of this thing and figure out what is going to work for us.

That was my takeaway. I think we can't rely on outside sources to give us these answers. We're going to have to come up with them ourselves.

JANIS KARKLINS: Okay. Thank you. Thomas?

---

THOMAS RICKERT:

I have to say I was quite disheartened by the session but I try to blame it on the jetlag. I guess the issue that I have in that gets back to the point that I made during the session. If you look at privacy policies on websites, the first thing that needs to be mentioned is who is responsible? Who is the controller? We don't have an answer to that. And a lot of the answers that we are trying to get up with here is we depend on that. It was my understanding after the first phase that ICANN worked beyond the steering wheel and start negotiations with the contracted parties to come up with data protection in whatever shape or form because we were not allowed to use the word joint control in our first report.

Now what I'm hearing – and again, I may have misheard this – is that these discussions are not taking place because we're waiting for answers. Answers that we don't know are and we don't know based on what assumptions, the questions being asked in the first place. So I'm totally unclear about with what mission the Strawberry Team is approaching the Commission or the Data Protection Authorities for answers and whether those are aligned with our policy plan. I don't know how to get around this because I think we do need ICANN Org to commit to a legal scenario that can be put in writing. I'm hesitant to believe that our group will be able to come up with conclusions in the absence of that commitment. How can we get to that commitment? I mean we've tried it for months and months. We got conflicting statements from the ICANN Board with Becky saying publicly we are joint controllers. And then comes the denial – we're not joint controllers, we need to assess this more. I don't know whether any analysis has taken place in the meantime. If so, I'd be interested in seeing what the analysis would be.



I'm wondering what so difficult about this? You can easily say that you are joint controllers. But if you say you are not and the court determined you are, you're in trouble. But if you say you are and you turn out not to be, you won't be in trouble. And I'm really looking for guidance from the contracted parties primarily because you're going to be part of the disagreement. Is there any way that we can move this discussion forward? Because it's my firm belief that we're not making as much progress as we could in this group because everybody is shying away from responsibility. Decisions shall be made [as well]. We want to be in control before disclosing data. We want the accreditation party outsourced. We want somebody else to be the controller. So it's all revolving around those basic questions.

And now we've heard that these are parked until some mysterious entity comes up and gives us the responses that we're looking for. And then whether we like it or not, there's going to be another question. The Commission has stated previously that they think we are joint controllers. It has not been accepted. So what are we waiting for? And what events need to take place so that we can expose [ourselves]? Now I sound frustrated and I am, but I'm asking this more or less out of desperation. How can we advance?

I mean I wrote five, six pages for the initial report, clearly laying out why I or the authors of that paper think that it is a joint controller scenario. What I think was a robust legal rationale, it was not accepted. Part of that was because the internal dealings of this group, part of that was by ICANN Org. So our group didn't come to closure on that. Then we said ICANN Org and the

---

---

contracted parties six months down the line were not a millimeter further than we are now.

JANIS KARKLINS: Ashley, please.

ASHLEY HEINEMAN: I'm not as frustrated as Thomas, but I admit, I had higher expectations for this session. At risk of sounding a bit mean towards ICANN, but it kind of felt like he wasn't as prepared of a conversation as [inaudible]. That was my impression. It wasn't so much that they were at odds with us, I just kind of – not to toot our own horn but we are more sophisticated in our discussions than they were. I feel like their conversations were kind of where they were maybe six months ago about what accrediting body could do or not do. I think we've gone past that.

So I'm not as disheartened about what was said. I kind of just took it for what I think it was which was they're just not up at the same level we are at this point. That being said, I think we do need to take a leap of faith and move forward in our conversations. We need to ourselves move past the chicken and the egg. While I do think that the questions that are being asked of the European Data Protection Board are ultimately going to be useful because it will tell us whether what we've done is bunk or not. At least we'll know at that point. If we have to change course, we have to change course. But at least we have shown that we have taken the initiative to go down a certain path, whether or not it's right, we'll find out. But I think what we need to accept and rather not ICANN

---

is doing this and doing that, when ICANN is doing this or doing that. At the end of the day, the responsibility is with us to develop the policy. They may be thinking something differently at this point but it doesn't matter. Our job is to develop the policy recommendation. I think we're going down a good path. We're not all in agreement yet obviously, but I think the conversations we're having right now on accreditation, we're actually getting somewhere. So let's just continue with that and take what little kernels we can from the conversation, but let's not get to downtrodden on what didn't hear and move forward.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I'm going to agree a lot with what's been said. I think I'm frustrated and much has happened since Marrakech. The fact that they couldn't even show the questions was simply astounding. So, I don't know. Maybe she's right. Maybe we just plod ahead and see what happens and see where we can go, but I do feel like – I was expecting a lot more sophisticated and developed responses. This seems almost like a brainstorming session at this point on their side.

JANIS KARKLINS: Thank you. Stephanie, once again.

---

STEPHANIE PERRIN: I just wanted to agree with what Ashley was saying and voice my concern that we do lose credibility if we're sending people in who are not up to the same level of sophistication because by this time, we should be further along. So why don't we invite the Strawberry Team to come to our session so that they can at least know what page we're on in terms of this. They may come up with a different set of questions based on a definition of accreditation that isn't anywhere near what we come up with, and that worries me. Thanks.

JANIS KARKLINS: Thank you. Dan?

DAN HALLORAN: Thank you, Janis. Just kind of uncomfortable in our chairs here because we actually work for Goran and we're here to support your team in whatever way we can, if you have questions for ICANN Org, we can take them back and consult with our colleagues. I'm a little bit confused and lost. I mean no one in ICANN Org I can tell you 100% has any idea that we create policies. We don't stop policies. We're here to implement the policies that are developed in this team and we're here to support you guys in the development, the support staff here.

Trang and I as ICANN Org liaisons had agreed 100% with what Marc Anderson said. It's up to you guys to make these policies. No one in Los Angeles here can make the contracted parties there do anything except you, this group collectively, when you make a consensus, you make recommendations that gets recommended

and approved by the Board and then the contracted parties have to follow that. ICANN can't make that happen by itself. ICANN Org can't make that happen and we can't stop it either.

I hear the frustration about the timing of the Strawberry. I think the Strawberry was never intended to hold you guys up or speed you along. It was like I think [inaudible] said earlier and a hypothesis that Goran had months ago that hey, when you guys get around to building one of these things, whether it's a hamburger or whatever, if you take that decision-making about who gets the data out of the hands of the contracted parties, they're not going to like that unless they're going to have a good idea that they're not going to be liable for those decisions. If someone else is making the decisions, they don't want to be at risk in making those decisions. So let's go ask the Data Protection Authorities. If you guys end up building a model that takes away that decision-making from the contracted parties and puts it in some centralized gateway or an authorizer, whether that's ICANN Org or some other authorizer under the TSG model, the contracted parties are going to go along with that or they're going to be so responsible for the decisions.

Goran has been saying for a few months they're not going to be interested in that. That's the whole Strawberry question which I think you guys are now kind of up to and with us. Trang and I are sitting here, we also work supposedly with Elena. We can take back any feedback or guidance. I'm just reminding you we're here and we're here to serve you and bring back any information or questions you have.

---

---

Just really quickly on Thomas's concerns, I'm happy to sit here and listen more. The jetlag wears off hopefully, we can sit and talk. But it sounds like the questions you have are about Phase 1 implementation. I'm having trouble understanding how that's related to the work this week, the Phase 2 stuff. I don't think anyone can decide yet until we know what the hamburger looks like and who's doing what, who would be the controller, who would be the processor, if there'd be joint controllership under a hamburger scenario, because we don't know yet where the party is and what are their responsibilities. I think first we have to define who's going to do what, and then we decide based on that who would be the controller, who would be the processor, whether it would be joint controllership for Phase 2. Thanks.

JANIS KARKLINS:

I really do not want perpetuate this conversation much longer, so I will take all those. The flags are up now. Fiona is one of them. That was on my list. Then I will take Alan, Stephanie, and then I will draw a conclusion, and we will move on.

FIONA ASSONGA:

Thank you very much. I think, Daniel, what you're trying to say here is that we would want to work more effectively with the Strawberry Team than being stopped. They can support us better. And what Ashley and Stephanie are saying is that they need to find a way of plugging into our conversation. One, so that they can understand what our concerns are, aware what issues are, and what kind of questions we need to pose. I don't normally talk much but sitting here today through the conversation, it sort of felt like

---

they were not so ready. They are not so ready for this audience. That's been very polite. They needed to come in prepared at least having listened to our previous meetings, if nothing else so they have an idea of what our expectations are, that their presentation is, if nothing else, up to par.

My suggestion? They should be coming in for our meetings even if [inaudible], let them have someone sit in so that they can hear what's okay. I don't know that they get their briefing but then you should have been the one giving the presentation. Thanks.

JANIS KARKLINS: Thank you, Fiona. Alan Woods.

ALAN WOODS: Thank you. I just want to get on the record specifically for you, Thomas, we are sitting down with ICANN about those agreements. I said this to Goran that we are mapping out. We, the registries and registrars, presented a document to them trying to map out what we believed and what we thought were the role of the data elements, everything. We have full data mapping procedure and we're currently back and forth on trying to agree that document still and it has unfortunately taken that long because again we're coming up against the same discussions that we're having and we're trying to work it through.

So, yes, I agree. It would be nice a bit more for an impetus. I completely understand what you're saying about – it would definitely help us in our conversations here if we know who the basic roles were. It would definitely help us in this because then

---

we would know who is the disclosing entity, who has the responsibility to apply 6(1)(f) balancing test where most staff and leaders naturally do.

So I have to say that we are doing it. It is slower than, unfortunately, I'd say we'd all like. But I think we do need to ramp it up. But again, there's a lot of capacity issues and things like that as well even though it is absolutely vital for the contracted parties.

JANIS KARKLINS: Milton?

MILTON MUELLER: Dan, we understand that probably policies or staff at your level do not think that they are making policy, that they are supporting policy process, and you probably are. I don't think that's true. I think there's a great deal of confusion at the CEO level and its immediate level. As I said, they have decided that they wanted to push in a direction of a centralized UAM. If you look at the amount of resources they have invested, they have created a Technical Study group and flown them around the world to work on it. Then they created the Strawberry Team.

I didn't want to be this blunt to poor Elena but I want to know why they even exist. What can they do that we can't do? We can present and develop questions to be presented to DPAs. We probably are in a better position to do that, so if this team has any rationale for existence at all, as everybody here is suggesting, and the message you need to take back is that they should be in here listening to everything we are talking about. And so far as they



---

have expertise that we don't on the nature of European Data Protection Authorities, they should be filling us in and talking to us directly and not working in parallel and refusing to tell us what questions they're going to ask of all things.

So, the frustration that you're hearing is justified. Again, I'm with Ashley in terms of spirit. I knew this all along. I knew that the CEO is creating parallel tracks that were not legitimate. We've been saying that from the beginning of the TSG. We should go ahead. We should make policy and we just have to get over the notion that we're going to get some special information from these parallel processes that we cannot figure out for ourselves to find out for ourselves. So I think we're fine. We'll just continue doing what we're supposed to do.

JANIS KARKLINS: With these words, Stephanie.

STEPHANIE PERRIN: Sadly I don't agree with my worthy colleague. I don't think we're fine. When I worked in the Data Protection Authorities' office and the entity came in to say, "Hey, we're thinking of doing this. What do you think?" And it's usually with a slide deck that told you nothing. So, eventually after what I call the dance of a thousand veils when you tried and tried to figure out where the beef was and the hamburger – I hate to use your image – I would ask pretty basic questions like, "Where's your risk assessment? Where is your privacy impact assessment?" Which is why I keep harping on

---

the “Who’s the data controller? Where are your Data Processing Agreements?” And if you haven’t done that then you’re in no way.

I think we run this huge risk that we are going to expose ICANN and the policy processes that we’re all here shedding blood, sweat, and tears over. Even if we don’t agree, we can at least agree we’re all working hard and we’re trying to get a product out of this that we can be proud of, right? We don’t want that blown by gathered and disparate processes that don’t hang together because we’re going at it backwards. Thank you. I promise I’ll shut up at this point.

JANIS KARKLINS:

Thank you for your assessment of the meeting. So what I take out of this that we’re condemned to continue, we probably would have gotten more information than we got that would be maybe helpful in our own work. Now we need to figure everything out ourselves at least for the moment.

From other side, I did not hear much contradiction what we are sort of discussing and then what UAM is about. For me, UAM is one of the options of SSAD, but there are many other options of SSAD and we need to find out what would be the one that all of us could say, “Yes, this is the one that we think is the right one.”

Therefore, I would suggest that we continue working on building blocks. We continue working on policy principles that have been outlined in the zero document and let’s see how far we can get by Wednesday afternoon. Then we will take this further with our online work until Montreal. And in Montreal, again we will see

---

whether we can get any more clarity from ICANN Org to determine the systemic elements.

The way how process is structured in my hand allows us to progress on building blocks without having a full agreement or determination on this intermediary phase. It would be good to have it but we can live for the moment without it. Hence, let's continue with our conversation on building blocks and continue with the one on accreditation. Yes, please.

GINA BARTLETT: Excuse me, this is Gina. When you say the intermediary, do you mean sort of the overarching architecture?

JANIS KARKLINS: The meat part of the hamburger.

GINA BARTLETT: Are people willing to do that to keep going with the building blocks?

JANIS KARKLINS: Probably there's no choice.

UNIDENTIFIED MALE: Always Disneyland.

---

JANIS KARKLINS: Okay, I will now pass the rein to Gina to continue moderation of the discussion on accreditation.

GINA BARTLETT: Earlier today we were breaking the accreditation into several components. One was around the purposes. And we talked about what some of those purposes were. Then we were going to talk about the policy requirements. Then we were going to talk about who would do the accreditation. Was it a one body or several bodies? Who might do the auditing function? And who would be able to monitor for abuse and do the revocation.

So we were thinking the next thing we would do is look to and talk about what the requirements would be for the accreditors. We had talked about one of the requirements would be that it would be certified by whom or by what policy. There was different ideas about that. There would need to be an ability to test the accreditor and there need to be an ability to be able to revoke that.

I'm sorry. I forgot. I feel like there was one component in your proposal, Milton, that was informative on the requirements. Do you recall? I wrote it down. I'm sorry but I don't see it. Oh, that was more on the who, the accrediting body actually.

So we were wanting to pick up that conversation. If you're able to do so to pick up where we were earlier today and talk more about the requirements that would form the policies for the accreditation.

Oh yeah, did you want to outline that, Marika, where we are with the building blocks and those requirements in there?

MARIKA KONINGS: Yes, thanks, Gina. I just want to put up what we currently have in there on some of these. Maybe we've already moved beyond that but I thought it might still be helpful to have this on the screen. Again, the first part here was more in general about the accreditation mechanism or what the expectations are. I think at least from a staff side of things, we've taken away some of the concepts that you've discussed here. So I think at least I feel comfortable in trying to write it up. I think it's partly as well what you're on the first sheet that you have up. I think the second part talks more about the accreditation process and the requirements related to that which I think it's probably more what you want to talk about now. So I just wanted to share that that's what we had in there as a starting point. Again, none of this may apply fully in your conversation here but it's probably worth seeing what's there and giving us some guidance on what the expectations are in relation to this part.

ALAN GREENBERG: I don't think we can separate the second column, on policy requirements, from the first item of the third column. That is, what kind of bodies are we talking about? Because the answers, I think are going to be different depending on the details.

GINA BARTLETT: Would you propose we talk about who the accrediting bodies might be first? What would you recommend?

---

ALAN GREENBERG: We could, or just merge it into the same discussion. People will wander back and forth anyway.

GINA BARTLETT: Okay, we'll just merge those together.

ALAN GREENBERG: Auditing and revocation I think are very detailed -iations, but the other top one is tightly coupled into how we write the policy.

GINA BARTLETT: Great. Okay. So, we'll jump in, then talking about the requirements that would inform the policy. You have a starting point in building block F of the document, and we can merge between who those accrediting bodies might be to help inform our thinking on the requirements. Okay? Did you want to jump in, or keep going? Okay. Volker?

VOLKER GREIMANN: Thank you, yes. Just one thought that occurred to me is that these requirements may be very different from group to group that is being accredited here. Because every single group might have different levels of access that they're getting. For example, if you have law enforcement of the same country that is being accredited, as the contracted party demanding is from, then they will have a very deep level of access, presumably, and therefore the accreditation requirements might be more stringent, and the consequence for failing in the requirements might also be more

---

stringent as opposed to a group that only has very limited access, where the requirements could be lessened and the consequences could also be less.

So I think we should have a scope here from within which we should operate and maybe just brainstorm ideas and then see which level of access, or which level of user group they would apply to.

GINA BARTLETT: Great. Do you have a proposal for any initial thinking on who the accrediting body might be, or what the requirements for them might be?

VOLKER GREIMANN: I think the who might follow from the various groups. A lot of groups would probably be self-organizing. I would think that there would be multiple accrediting bodies, simply because of the necessities of having a certain amount of information on the group that you're accrediting. However, that's something that would probably be open to the marketplace. We've seen the various proposals out there. The proposal proposed by Deloitte set might be a model for something. I'm not saying that that is the one that we should end up with, it's just a model that we should look at and therefore see how we can develop from that. You've heard various suggestions like WIPO and INTERPOL. They might be interested parties, but they might not be interested in doing that after all. By saying that we want WIPO to do that, we might just [lay an act] that we cannot hash.

GINA BARTLETT: Thank you. Okay, I've got Alan G., Brian, Milton, Alex, and Chris.

ALAN GREENBERG: Thank you very much. I guess this follows on from what Volker was saying. With the possible exception of WIPO, and it's a possible exception, I cannot think of a single other group of people, for whom there are bodies existing, who could do accreditation around the world. Even if you look at the relatively simple case of lawyers, and intellectual property lawyers, they tend to be done on a national or a state-province basis, and certainly not on an international process basis.

INTERPOL, which was used as an example, I think, doesn't work, because we're not going to be willing to treat all police forces internationally identically. Security don't exist at all, security professionals, and it's hard to imagine how one would create a group that could accredit around the world. I think we're going to be stuck, at least on a moderate-term, with doing accreditation on local bases, and having lots of them, unfortunately. Thank you.

GINA BARTLETT: Thank you, Alan. Brian?

BRIAN KING: Thanks, Gina. I think I might be able to unstick us. I think the answer is, we don't care who. I think the answer is that we should build out the requirements that it'll take to become an accreditation



---

body, and then come one come all. You build it, and if folks are qualified and can meet the requirements, then they could become an accreditation body, and if they can't then they won't. I think our policy work here is to set up the parameters: the entry level, the threshold that an accreditation body would need to meet. If an entity comes and they wanted to become accredited, then they could do that. Thanks.

GINA BARTLETT: Milton?

MILTON MUELLER: Yes, I want to make it clear that I'm totally against the whole idea of multiple self-appointed accrediting bodies. I thought I had made that clear in the morning. I thought that we had established in the morning that the only thing that accreditation gives you is some kind of traction on the identity of the claimant, and that that identity is most relevant in the cases of law enforcement. I would be amenable to some kind of a law enforcement accreditation thing, but the idea that we're going to have a set of general requirements for anybody to come and declare themselves an accrediting body is transparently a nightmare that, again, requires ICANN to accredit each accreditor, and it institutes forms of auditing and review of them which is just ... They may as well be doing the accreditation of the people themselves.

The accreditation process, in my mind, is much simpler if you don't base it on user groups. Again, law enforcement has a special status as a user group. Possibly trademark holders do, but

everybody else is basically just saying, "I've had some harm that's related to a domain, and I need to find out who the person is." You can ask what the particular basis of that claim is with a general uniform accreditation process that signs an acceptable use policy. Do people really understand what they're getting into by having this be open-ended, and having the Indian Association of Religious Groups accrediting people who want to take down the anti-Hindu websites? This is just a crazy idea, insofar as we have a track of people who have some kind of automatic status of having access to disclosed data. It might be law enforcement, and I think we'll have enough problems thinking about how to crack that nut.

GINA BARTLETT:

I have a lot of people, a lot of cards went up on that. I'm going to go Alex, Chris, Janis, and then I have Dan, and then I have about four or five more people, which I'll get to. We've heard on the who, we've heard WIPO, then this concept around multiple entities; we're just relying on the requirements and concerns about that, especially because that makes ICANN required to do the accreditation. If you could speak to that, and try to bring us to problem-solving space, that would be great. Alex.

ALEX DEACON:

Yes, thanks. Again, I'm just quickly supporting Brian, that I think the "who" question can be answered later. We shouldn't get wrapped around the axle around "who". I think we should focus on the requirements. To address a few things that Milton said, at least one, I think we need to set a policy. If you remember my

---

diagram, that was the box in the lower left-hand, with the trusted accreditation program policy, that describes the policy about who can be accredited and who cannot. If there are concerns, as you expressed, then the policy can be set accordingly. That would ensure that we don't have 1,000-odd obscure accreditation bodies in the system. We as policymakers set the policy as to what requirements are needed for accreditation bodies to be let into the system. I think that can be managed; at least, that was my hope when I cooked up that policy in that box in the lower left.

Regarding requirements, and how we should start; again, I think we should think about these common, or what I call baseline, requirements. These are requirements that all accreditation bodies should have. We should at least start with that foundation, and then once we've done that, I think we'll have a good starting point for the policy about how bodies could then leverage that, and apply their specific requirements for their specific user groups. Those are my thoughts about how we should move forward here.

GINA BARTLETT:

Okay. I'm going to go to Chris, Janis, and Dan. I still have to get to Dan. We're talking very process-y, and since you have a start in your building blocks on requirements, maybe as you make your comments you could add to, or make suggestions to, the requirements as well. Chris?

CHRIS LEWIS-EVANS:

I think we've got two documents that already detail a lot of the requirements we already have. We've got the use cases

---

documents and Alex's one that we received this morning. I think any accreditation platform has to detail some of the safeguards that need to be put in place, and that the requestors need to agree to. That sort of talks to what Alex has just been saying about the baseline policy getting signed up.

Realistically, we have to baseline policies in this diagram. One is for the accredited body, assuming we have more than one, and the other one is for the actual requested. In that is also, from the use case stuff, all the safeguards that we've been working on for the last who knows how many hours, and all the other requirements for that. Realistically, for me, they are a lift-and-drop into this. I think that's the whole point of us doing all of that work, is so we can use slides of that. I think it would be a waste not to take that opportunity to reuse some of our work.

That's it for me on some of the requirements. I think we don't need to lose sight of some of the point of, just because the entity has been accredited, that their request might be denied. We mustn't lose face with that. Just because it's a police force from China doesn't mean that their request's going to get through. It also doesn't mean that their request will automatically be denied. That is a decision based on something else. That is, in my mind, separate to accreditation. We've not lumped in accreditation and the request together yet. We are just talking about accreditation here, and for accreditation I don't care if I go in, I can still ask for a stupid one and it should be denied. That's not what we're talking about at the moment, so I just ask that we don't lose focus on that. We're looking at how we accredit people, not how we do the balancing test, or how we check if the request is truthful or not.

---

---

We cover that a little bit in safeguards. We're saying that they must do truthful things, but we obviously have to test that at some point.

Really, that's what I wanted to do on requirements. At the end of the day, there has got to be one person that accredits the accreditors. I think Alistair Milton said you can't just have Tom, Dick and Harry turning up as accreditors, it's all got to be checked. I heard what Goran said earlier, and having very brief knowledge of Article 42/43, I personally probably need to read up on that, but that's not the right framework for us to do accreditation on. Even if we stick to the guidelines in there and they don't get signed off by country, I think the DPAs or the ePDP will look at that process and say, "Actually, you've taken the best practice and you've done everything right."

I think, going back to an earlier conversation about what they can and can't do, we shouldn't rule that out. They should be able to present that to the European Commission and the European Data Board, saying, "We're an organization outside of the EU, however we know we're processing European data, and this is what we're doing in line with your recommendations." I can see us having a single body, and then having a very small number, maybe contracted out, maybe coming back down to one. I can't see hundreds working, because it's just not scalable. It really doesn't work. From a requestor point, it doesn't work. Who do you go to? If you get told no by one, do you go to someone else? Probably, from the contracted parties side, they don't want lots of agreements as well. For me, I think we really need to limit that group of accredited bodies. One is obviously easy but may not

---

work. We may need some contracted out, but I think we need [inaudible]. Thank you.

JANIS KARKLINS:

Thank you very much. I want to make two points. I also share the view that we need to think of a limited number of organizations that do accreditation, and in this respect the user groups most likely are useful in order to cluster potential users according to certain principles, and then associate that particular user group with the accreditation body. We heard today two examples ... I think it's Europol, rather than INTERPOL, that Goran was talking about, and WIPO, and answering a question or doubt that will express whether they would be ready to undertake that role. From a CO, I understood that he has preliminarily asked the question, and organizations expressed their readiness.

Myself, knowing the Director-General of WIPO, I asked him a question whether WIPO would be willing to engage on accreditation, should it be asked, and I also received a confirmation from the Director-General, without further details. Cost will be involved, for sure, and process will be developed based on what requirements will be put forward. That's a simple point of clarification.

GINA BARTLETT:

Dan?

---

DAN HALLORAN:

Thank you. I've got a little bit of confusion. Trang and I are trying to confer. You're talking about accreditation, and we are starting from the concepts in the technical steering group model of ... I think it was authentication and authorization? There's three different concepts, and authentication to them, just in their model, I'm not an expert on their model, maybe we could go back to that ... Yes, I'll speak up. Authentication was basically, "Who are you? Are you really a police officer? Is the person that I'm talking to really that police officer?" That's the authentication set, which is separate from authorization, which is, "Okay, fine. Now you're a police officer, and you really are the police officer you say you are. What data can you get under this policy?"

It's not clear how the accreditation covering both those cases ... I heard Alan G., for example, talking about that that wouldn't work, because they might know who's a police officer. That's the authentication, but not necessarily ... Just because you're any police officer anyway, you might not get all the same data as any other police officer, and that's an authorization decision, deciding who gets what data, which comes after authentication. Accreditation, I guess, is a different concept which I'm not clear how it matches over those two concepts from the TSG report. Thank you.

ALEX DEACON:

I think we touched upon this. Hadia asked me a similar question this morning. It could be. Again, these boxes are pretty high-level, and still to be defined. It could be that both the authentication and the authorization function, if you will, happens in the accreditation body box. Basically, it is the job of the accreditation body to vet

---

enrollees, issue credentials, which they will then use to be authenticated to the SSZ systems, and also the authorization part could be part of that same box. That's how I see it. I think we do need to think about that and flesh this out a bit. I don't know if that helps. This is how I see it in my mind, but there may be other ways to do it.

GINA BARTLETT:                   Okay. Marc A.

DAN HALLORAN:                   I just think, since I proposed an alternative model to Alex, I want to say I don't think those two things should be bundled. The only thing that accreditation can give you is authentication, and in most cases it cannot give you authorization, it's very clear.

MARC ANDERSON:                Thanks, Gina. The reason I originally raised my hand ... I think I've been overcome by events a little bit, here, which is fine. I think we've had a really good discussion here. Milton teed this up in an e-mail yesterday, pointing out that coming into this we all probably have very different ideas on what authentication means. I think Dan was touching on that a little bit. What does it mean when we talk about accreditation model?

I think this is a conversation we've been needing to have to get all of us on the same page, as far as, "What are the policy recommendations we need around accreditation?" There's probably a general feeling around the table that some kind of



---

policy recommendations around accreditation can be helpful. I think this is a great conversation. I'm glad we're getting to the point where we can have this conversation, but my takeaway is that we're still very much in different places, as far as what the benefits are and where we can go with this. As I was listening to everybody, I think Chris, Alex, Milton, you all had excellent interventions. Dan made a good point.

One of the things I'm wondering, and this maybe is something we can consider for homework, or a future discussion, is maybe some of the groups ... SSAC, you, of course, represent groups that want to get access to the data. IPC, GAC, you sort of represent law enforcement to a degree, here. Would you be able to take homework back and say, "What would your perfect accreditation model look like for the groups you represent?" We don't want to have too many different models, but I'm not sure that one model will cover all of us. If we looked at just for specific user groups, for specific groups of people accessing the data, would you be able to come back with a proposal or presentation for what you think that model should look like?

I'll pose that beyond to the rest of the group. Would that be a way to help us move forward on accreditation? I'm not saying that to stifle the conversation here. I think this is a great conversation that we've been needing to have, but how do we move forward to the next level? Just some thoughts.

GINA BARTLETT: Thank you, Marc. Stephanie? I have Stephanie, Alan W., Alan G., Mark Sv., Hadia, and Ashley.

STEPHANIE PERRIN: Thanks. I just wanted to say that the reason why our research group, that's the University of Toronto and the University of Ottawa, are still looking at data trusts as a model here, independent data trusts, is that we don't actually think there is any way that you can accredit and then process the requests. We don't think ICANN is in any position, as the guys who run the domain name system, to discriminate between a Chinese government request and a Canadian government request. It, therefore, has to be turned over to an independent body, and that's also the only way to deal with the myriad of potential user groups. You cannot, in a watchers watching the watched ... You know the one I mean. It's this quote, whatever it is. Yes, thank you. You can't hand over the determination of the police request to the police agency, or union, or authority. They have to go to a judge to get a court order, right?

It's the same thing here. There's a chasm between Alex Deacon's model, and I think Milton and I agree on this one, and what we see as the necessary distance between those who authenticate, "Yes, this guy's a cop," and then deliberate on the request. The more we ambiguate this, the worse we get. We've got to get our definition straight early on. Thank you.

GINA BARTLETT: Thanks, Stephanie. Alan W.?

---

ALAN WOODS:

Thank you. Both Stephanie and Marc made my brain change twice in the last five minutes, so I'll try and pull it together very quickly. Again, noting the path which Goran was mentioning earlier, where it seems clear that ICANN don't want to be this person who audits the auditors, or becomes that auditing of the accreditation body, that's fair enough. We have to come up with something, and I think we're going to absolutely twist ourselves into utter knots of, we're the people who need to set the process here, as to what do we expect from accreditation. With a bit of hybrid of what Marc was saying, I really think that in order to prevent the floodgates from occurring, we can't say, "These are the criteria you need to meet in order to be an accreditation body." I think we necessarily need to set up a policy that, "If you want to become an accreditation body, then you need to come to us with a fully baked plan that we can look at on an individual basis. We have to set a consultation, we have to look at it specifically." We're not just asking that we think we can verify this, it has to come with some sort of official ... I don't know, I'm trying to figure it out.

Again, from a European point of view, somebody who's gone to the DPAs and they've green-lighted and said, "Yes, this would work from an accreditation point of view, we would be happy that the responses that came from this could be more biased towards disclosure because of this accreditation." You have to come fully baked with that, but also not as a basis of the requestors. I think that's a really dangerous road to go down. We shouldn't be going down requestors, we should be going down legal basis route.

I'm very sympathetic to the law enforcement basis. From a 6(1)(c) point of view, it should be relatively straightforward to say, "I am a

---

particular law enforcement official in this country, and I'm going to be relying upon this law, and this power which I have." There should be a method of which you can come up with. It's not saying that you should get accreditation, but it's just verifying to the person who is ultimately disclosing that they are from that jurisdiction, that there is this power from that jurisdiction, and that you are subject to that jurisdiction. It's a clearinghouse, more than anything, of whether a law applies to a certain discloser, in that instance. But that will be different for something that's under ... You're not going to get an (a). Well, I don't know you're going to get an (a). A 6(1)(f) is a completely different concept, because I don't know that it will be as straightforward.

There would have to be an awful lot. We've heard from both ... God, I can't think of the names, now. It's the two people who presented. Deloitte and WIPO, isn't it? We've heard that they're people who can help in that process, and perhaps we need to bring them into a conversation at some time to say, "Well, what could you actually do to help in that accreditation?" Again, the fully baked comes to us. I really think that we cannot be the people who set the requirements for accreditation, because we're going to end up a floodgate, we're going to hand over people who shouldn't get accredited at all, and I don't think we're qualified to make those calls. We can expect or not, but I worry about it, to be honest.

GINA BARTLETT:

When you say "we," do you mean the accrediting body, or "we" as in this group?

ALAN WOODS: No, we shouldn't be creating policy about what is an accreditation, because I don't think we're qualified.

GINA BARTLETT: I just wanted to confirm the "we." Thanks. Alan G.

ALAN GREENBERG: Okay. It's difficult being after such a long queue. A couple of things. First of all, I was wrong before when I was talking about INTERPOL, or Europol, that I was, as Chris pointed out, conflating the decision on whether to release information with accrediting. Foreign law enforcement is almost surely going to be one of those that will have to drop through the pile; what I was calling an escape hatch, before. The contracted party, perhaps based on some table their own law enforcement gives them, decides whether this foreign country are friends, and we trust them, and this one is ones we don't. It could well be automated at the contracted party level, but it's certainly not going to be made at a global level. I'm sorry, I conflated that, and that was my mistake.

In terms of who does the accreditation, and back to Milton said; we should do it. Like the balancing test, accreditation may well involve judgment calls. You may meet the paper criteria, but you may be deemed, for whatever reason, to be not ones we want, or ones the accrediting body wants. Accreditation, we have to presume, will include some level of human intervention and decision on whether person A is in fact someone we want to accredit or not, and trust or not. It has got to be done at that level.

---

I half agree and half disagree with Alan on the fully baked versus us setting requirements. I think we have to set some sort of outlines. We have to say what kind of things we're looking for. Yes, if someone comes to us, then I think in most cases they will have to come to us. But, if we reach out to them and propose they make a proposal, fine. It doesn't have to be purely on their own volition. I think it has to be a combination of the two.

Bottom line is, I think the people who want access are going to have to group together and find entities that can accredit them, because they're the ones, ultimately, who want the access. It has already been said, but it's not a matter of anyone who declares themselves to want accredited people to accredit them. It's got to be within certain overall ...

We've been spending an infinite amount of time on use cases, and we have use cases for many of the class of requests we think might be something we can handle through this kind of system. I think that's the start of it. There may be some ones we didn't do yet, but I think we're well on the way of identifying which groups of people that we may think will fit the model, and which won't.

GINA BARTLETT: Mark Sv.

MARK SVANCAREK: As Alan says, it's been a long time in the queue, and everything's changed a million times. You've all said many thought-provoking things. I recently put up my hand because I was thinking that Milton's intervention about user groups had something to do with

---

Alan G's concern about police forces, namely that if you're thinking about user groups, and that there's an accreditor that allows in all the people in the user group, that that's a terrible system, whereas if you have a bunch of people who come and try to get accredited by an agency, it's because they have a similar set of bases and a similar set of qualifications. They're not really people in a user group, they're an atomic collection of requestors who simply have some shared attributes. I think Alan W. said something along those lines as well. Again, just dispensing with the concept of user groups seems like a good idea at this point, whether we share the same bases or we share other attributes, but not because we're all IP lawyers, or something like that.

Alan W's other idea about ... It's just sounded like the endless chain of turtles all the way down. The accreditor of the accreditor of the accreditor. But ultimately, we know there is an official formal way to do it, where there's a route of trust, which is the DPA. How far down the chain of turtles we go before it's moot, I don't know. I did say earlier that I thought that we should start this process. We should make some sort of a concrete effort to do it, but ultimately expect that there's a formal thing at the end of the road, which is a code of conduct that is approved by the DPA, and a monitoring body that is approved by the DPA to enforce that.

Last, to Marc A., I think there have been some draft accreditation and access models that were put together a year or a year and a half ago, and maybe people could look at those and see if they're still applicable to what we're talking about. Rather than starting from scratch and a piece of blank paper, there are probably some things that people could build on right now in order to do that

---

---

homework that you asked them to do. Gosh, I hope that was useful. We have all been in the queue for a while, and I got a little bit lost.

GINA BARTLETT:

Thank you. I know everyone's been in the queue for a while. It's interesting. Just while you were talking, I was looking at building block F, and a lot of what's being discussed is referenced in there. It's pretty similar, with some modifications, maybe some additions. I just wanted to point that out while we keep talking. Hadia, Ashley, Margie, and then Greg.

HADIA ELMINIAWI:

I'm not sure that we will be able to talk about the "who" right now. My original thought was this part would be requirements, and then after finishing the requirements we look at them and then start discussing this very difficult question about "who." I would add a policy requirement that the accreditation body should have the ability to carry on specific assessment activities to make sure that the accredited entity meets the requirements.

Then, there was this discussion about accreditation and authorization. My thought was that right now we are talking only about accreditation, and right now we're not talking about authorization. Authorization will ultimately depend on the identity of the requestor, because you would have a requestor with a specific purpose that requires access to specific types of data. Although authorization will depend on the accreditation, right now



---

we are talking only accreditation, and let's keep authorization out of this, now. Thanks.

GINA BARTLETT: Thanks. Go ahead, James.

JAMES BLADEL: No, that's okay. I'll pass. Thank you.

ASHLEY HEINEMAN: Just a few sweeping comments, because I'm getting a bit tired. Just to agree with some of the things that have been said, including Alan. I don't think we need to find ourselves in a situation where we have to go into extreme detail about requirements for accreditation. I think we're more at high-level principles, that sort of thing, recognizing that GDPR calls it out too so we can point to that. I don't think we need to spend a whole lot of time mapping out specifics.

Also, when we have these conversations there are people who do accreditation for a living out there, so perhaps we need to build off of what services are available out there, rather than ... Well, WIPO might be a great example, and they might be willing to do it, but my guess is they're going to be partnering with an accreditation body. Just to put a very fine point on it, because it keeps getting brought up as an example, Europol and INTERPOL will not be an acceptable solution for a law enforcement. There's very different national sovereignty issues, so if we could stop using that as an example, I think that would be helpful, because

---

we're perpetuating something that's really not going to be possible. Thanks.

GINA BARTLETT: Thanks, Ashley. Margie, thanks for waiting.

MARGIE MILAM: Thank you. I agree with Ashley. I think it's high-level accreditation principles we want to talk about, because we don't want to be too prescriptive in what we need. Give WIPO as the example. If WIPO becomes the accreditor for IP-related interests, I imagine the contracting process is going to be very different with a UN agency than there is with a Pricewaterhouse, or something like that. Can they even give indemnification? Is there unique issues because of who they are, that might not be able to live up to, or not be able to sign up to, the obligations we might have? I just want to think at a very high level.

The other thing too, a group like WIPO, and I know we don't want to integrate INTERPOL, but something like that, what's the likelihood they're going to be sued if they gave an accreditation when they weren't supposed to? I have a sense that it's probably less likely than a normal, private corporation. Again, I think that coming up with high-level principles, and not be too prescriptive, because we want to encourage that kind of creativity. If WIPO's willing to step to it, that's great. Let's give ICANN the ability to [fix a track] with them, in whatever form that they need to, to have a relationship.

---

GINA BARTLETT: Thanks, Margie. Greg? Thanks for waiting.

GREG: Thank you. We're trying to comply with the law to figure out an acceptable solution, and we need to look at the law itself, where it provides guidance. I think, as a group, we could do well to study articles 42 and 43 some more. We haven't really discussed them a great deal. They seem to provide a lot of guidance. They're about certification bodies, and they tell us what those certification bodies are, and what they need to do, and in some cases how to do it. There's a clause that tells us about how you solve conflicts of interest. Maybe we should look at that more, because we don't need to reinvent the wheel if the law tells us we have a guide here that we should look at.

As far as groups of users, I think they were useful sometimes because they let people think about the use cases that people had, but they're also ... I think that anybody who's going to get accredited is going to have to satisfy some common requirements that are going to be the same for whatever you are. Sectors tend to break down. Some companies, for example, like a Mark Monitor, they deal with phishing one day, and they deal with an intellectual property protection issue the next day, and maybe something the third day. Which sector are they in? In a lot of ways, it doesn't matter so much who they are as, are the requests they're making being made under legitimate purposes?

The groups break down, and it strikes me that there are some bodies out there, like Big Four accounting firms, who can understand the use cases across sectors, and can understand

---

what it would take to accredit people in more than one industry. That might be a solution, rather than trying to break things up by user groups, which seems like an artificial thing in the end, to me. Thanks.

GINA BARTLETT: Thanks, Greg. Alan G.?

ALAN GREENBERG: That was an old hand.

GINA BARTLETT: Oh, that was old. Milton?

MILTON MUELLER: Let me try to summarize. It seems like there's some progress here in the discussion that could be encapsulated. I think the number one ... Ashley has said that Europol and INTERPOL are out of the picture as possible accreditation agents. That seems to be a fact, okay? If we're talking about accrediting one of the most important types of entities, law enforcement, we really have an issue as to how that's going to happen.

Secondly, I think we've agreed, though I'm not sure, that accreditation will pertain to authentication and not authorization, that bundling those two things creates serious problems of incentives. For example, we think of these accounting firms, which is not a bad idea. We don't want them selling accreditation as a cheap and easy way to get access to data. That touches on my

next point: most of the discussions of accreditation have talked about how or who to accredit, but they have not at all talked about how to de-accredit agencies that are abusive or fly-by-night, or not doing a good job. Again – I see Alan W has left, but he seems to be convinced that ICANN doesn't want any of these responsibilities. I don't care whether they want it or not, I'm, as a policymaker, willing to give it to them if they're the best party to do it.

Another point that we seem to be omitting is, can we agree that there will be a track for the unaccredited? Or, are we saying you have to be accredited to be a user at all? Maybe this is a slower track, maybe it's more manual, but can we agree with that, that there is a track? If there is a track, just as an empirical question, do we think that the number of requests from unaccredited parties are likely to outnumber those from unaccredited sources? Maybe I should say the number of sources would be large, maybe the number of requests would be smaller per unit, but what kind of quantities do you think we're dealing with here, in terms of – we're so focused on the big categories like law enforcement and WIPO, but if we agree there's going to be an unaccredited track, how big do we think it is? Therefore, we really need to think about how to do it, which is something I don't think we can ignore.

GINA BARTLETT:

Milton, when you say “unaccredited track,” you mean unaccredited entities that might want to come forth and apply for accreditation?

---

MILTON MUELLER: Exactly.

GINA BARTLETT: Thank you. I'm sorry, to become an accrediting body.

MILTON MUELLER: No, that they would want to use the system to disclose data. So, I'm a small business owning a trademark in Des Moines, Iowa. I'm not affiliated with WIPO, I don't know anything about that. I just see somebody using my trademark, I want to find out who it is and sue them.

GINA BARTLETT: Thank you, I think I was the only one who didn't get that. Thanks for those summary points, Milton, and potential areas of agreement. I have Margie, and then I'll come back to Brian.

MARGIE MILAM: Yes, I agree with Milton that there should be a track for people that are not accredited, and that could be more manual or whatever. Not everyone's going to fall into a category. The accreditation is for large, whatever, groups, legal basis, whatever you want to call it. It's a way to facilitate the access. The reason I raised my card was because the question about Article 43 or 44 of GDPR applies. I think it might be a red herring for us, at least according to Goran, if I understood him correctly, that's only done by a government. The government identifies who's going to be certified. I don't know how that would work. Are we saying that a

---

European government would certify a PWC? I don't know, it doesn't seem very likely to me. If we could get clarification on that? If that's the correct interpretation of that article, then I don't think we should be referring to that article, unless it's purely for guidance, like Greg was saying, to help at least think through what the issues are, but not in terms of actually getting formal certification to be an accredited party under GDPR. Thank you.

GINA BARTLETT: Does anybody have an answer to that, to Margie's question? Chris, do you have an answer?

CHRIS LEWIS-EVANS: We might tag-team on this with Georgis. It refers to a competent authority, and I am literally just going through it myself. It doesn't need to be a country, but it has to be a competent authority. Goran was pointing out earlier, to be a competent authority you have to have some legal basis, which is where that stumbling block is. You don't need to be a country, but you do need to be a competent authority.

GINA BARTLETT: Thanks for that immediate clarification. Brian, to you?

BRIAN KING: Sure, thanks. I'd like to keep building on where I think we have some agreement. There's a couple of things that Milton noted that I'd like to agree with. One, that we think there should be a track for

---

unaccredited parties that can still use the SSAD to request access. We agree that we also could recommend what ICANN's role should be in this, because Goran's a little uncomfortable about how it might work or ICANN's current expertise in it. I think that's fine, I don't think that any policy recommends they do it anyway, with the right policy recommendation.

I would potentially disagree with Milton on the concern he expressed about rogue accreditors, and I might suggest that we could address that concern if we focus work here on the requirements it would take to become an accreditor. I think if we're smart about what it takes to become an accrediting body, we can really alleviate those concerns. Things off the top of my head are to post a bond of a million dollars, or whatever threshold of membership you might have, or having access to whatever the data's going to be used for. There's a number of things that we could build in that would really hopefully eliminate, but all-but eliminate the potential for abuse by rogue accreditation bodies. Thanks.

GINA BARTLETT:

Okay. I know we're getting shorter on time, but can anyone speak to your thoughts around the revocation, how to do that? I think someone earlier just said that they thought that that maybe should be an ICANN cap. How do you about revoking the ability of an entity to provide accreditation? I just thought it would be good to hear what people's thoughts are about it.



---

**BEN BUTLER:** It absolutely has to exist. One of the updates, if I make an update to my slides earlier, would be that the box labeled “trusted accreditation body program policy” will be defined as how they're approved into the system and then how revocation can happen, and under what circumstances. I think again that policy would be spelled out there. It's an absolutely important that if you're going to onboard folks and approve them, you need a way to kick them off the system.

**GINA BARTLETT:** Thanks, Ben. I have Volker.

**UNIDENTIFIED MALE:** Thank you. Just as a general principle, what we're essentially talking about is making sure that there's an effective feedback loop system built into this. Feedback loops are designed and integral in lots of different types of systems, and the core principles are that both parties who are directly involved, as well as third parties, have the ability to question the legitimacy of a particular transaction, and that the parties involved can have a mechanism to investigate and produce reports and documentation, something like that, within a reasonable timescale. In this case, the registrars and registries think that somebody isn't or shouldn't actually have access to the SSAD, they can kick that off. If the data subject gets notice that their data was disclosed as a result of the SSAD, they should have the ability to complain to a controller or a process within. All that needs to just feed into a loop that moves literally circular.

GINA BARTLETT: Volker?

VOLKER GREIMANN: Yes, I also think it's important that this process ... Back at you ... That there's a process for the accreditation or decertification, or whatever we end up with the terminology. For example, if a certain party is an accrediting party that are leaving to [pull on] some data, disclosure complaints, or somebody is finally convicted or fines for a disclosure made to a party that was accredited through a certified entity, then there should be consequences.

On the other hand, I don't want to end up with a situation where you have to accredit such a party, and suddenly all IP lawyers are without an accreditation vehicle anymore, so that's something that we also have to consider, that there should probably not be a monopoly on these operators.

On the other hand, it should not turn into a wandering circus, where one certified entity is being accredited, the next one opens up shop in the next town and does the same thing again. There needs to be certain safeguards also for what happens after such a party has been certified. Who can take up that mantle afterwards?

UNIDENTIFIED MALE: Volker's kind of blown my mind there, as opposed to blowing his nose. Sorry. It's just this huge can of worms, as Volker was pointing out, there. I think when we're talking about feedback loops, it's silly to assume that a person who has an issue with their

---

data being sent out will complain to us as the register complains to the accrediting body. They're just going to complain to the DPA. I think the difference between having a green light from somebody who's DPA accredited, looking there to Article 42/Article 43 type things, versus something that we ourselves are going to be auditing or reviewing, or taking into account. If somebody who was accredited by us, per se, if somebody has a valid complaint to the DPA, but we process that data incorrectly, that bring down the entire accreditation, because we must assume that the safeguards are no longer sufficient for that accrediting body. Not just that accredited entity, that entire accreditation body. That's a huge thing.

However, with a DPA [inaudible], we can say, "Well, you've still given them the green light. It's still a certified body updating your certification." Again, it's the layers of where we need to interfere, and where we need to actually audit and keep an eye on the accreditation body, as opposed to, we can just rely on the fact that they've gotten this green light from an official source, again, we must take into account the risk of de-accreditation on that as well, and just how would we handle that? I genuinely don't know how we would handle it.

ALEX DEACON:

You're right, these are big questions. If you remember, I mentioned that my framework was based on one that exists today. Maybe over a beer I could tell you the horrible story how one of the biggest certificate authorities on the planet was removed from the root store of every single browser on the planet. That was a huge decision, with consequences that were global to every single

---

Internet user. I could tell you that story, but that aside, if our process and policy is clear, that these are the requirements you must meet, and also for de-accreditation – I think that’s the right word, Volker – these are the things that will get you de-accredited, and we’re transparent and it’s clear, and when events happen we could point to the process that says, “We are kicking you out for these reasons. You will always need to do a risk analysis to make sure that the impact to the users are considered.” Then again, I think we have a good footing. We’re not making these decisions based on feelings, we’re making them based on policy that we’ve set. Yes.

GINA BARTLETT:

Maybe we should check-in where we’re at with accreditation? Is everybody winding down? You’re out of ideas? Are you? Margie?

MARGIE MILAM:

I have an additional thought on the de-accreditation concept. It doesn't have to be all or nothing. With the RAA, there's graduated sanctions, and there's some ... It obviously need to be well-defined, and all of that, but there could be a series of steps, especially if you're talking about de-accrediting a large group of trademark holders, or WIPO or whatever. It doesn't have to be all or nothing, it could be graduated sanctions and some sort of penalty before it actually gets revoked. I think we should at least consider that option.

---

MATT SERLIN: Sorry, one thing. Alex, while you were talking, when we were talking about de-accreditation, if not ICANN then who? As much as I love you all, this group cannot stay together forever. I mean honestly. Come on, now, really. Unless we appoint another body to – both bodies that want to do accreditation, and then de-accredit, if not ICANN then who?

BRIAN KING: Thanks, Gina. The answer needs to be ICANN, and if nothing would stop ICANN, maybe we shouldn't stop ICANN from pulling some help to audit and that kind of thing. They could certainly outsource it. I think instead of calling this topic of conversation de-accreditation, we can call it remedial action or things like that. As Margie said, maybe there's some throttling at first, maybe there's an investigation, maybe there's opportunity to cure. There should be steps that are taken prior to de-accreditation. Maybe we'll rename the concept here to remediation or something like that. Just making a glib comment while Matt was speaking – sorry about that, Matt – artifact of a long friendship. Probably I shouldn't sit next to you, that's the trouble.

To elaborate on that a little bit, I came into Los Angeles thinking accreditation was just one of the items on our shopping list, we had to get that put away. All I've heard in the last hour is this is way more complicated, way more onerous, and a heck of a lot less useful than I thought it was coming in here. So, why are we doing it? We haven't even demonstrated that we have a volume problem yet. We haven't even demonstrated that the hole that accreditation is meant to plug exists.

---

I think that maybe we ought to take one step back from all of the minutiae of how it works, and just ask ourselves again: are we sure we need it? You've already completely talked me out of any automated approach, so now everything has to be reviewed manually, which doesn't necessarily mean it needs to be slower, because the volumes that we're seeing on existing systems that are running concurrently now, even for large providers, are in the single digits per day.

ASHLEY HEINEMAN:

No offence to you, but that was a real downer comment for the end of the day. I thought we were making really good progress on this, and if the whole intent here is to bring efficiency into a process, this is a way to do it.

A comment on the volume, the volume might be low now because there's an education problem out there right now. People don't know what they don't know. By saying volume is low now does not mean there is not a need for the information. I think we just need to be careful when we talk about not getting as many requests as you thought you would. It's because people don't know how to get the information they want. They don't understand that a change has been made to the WHOIS, that that's why all the information's been redacted. I just think we need to be careful with those kinds of statements.

I think, before we say that you've heard nothing that's of value for accreditation, maybe something we can do as homework is put down in writing, "What is the value of accreditation?" so we can get past that comment. I think it's a fair point. We've skirted it the

---

whole conversation today. If we can just articulate that, then we can move on.

GINA BARTLETT: Thanks, Ashley. Margie, Mark Sv., Alan G., and then I think we need to check in.

MARGIE MILAM: I was going to say much of what Ashley was going to say. There's just an education issue out there. I'm also on that INPA WHOIS Subcommittee. We see a lot of confusion even in the IP lawyer space, and people that go to INPA about how to make requests. And then the other thing from a company that does submit a fair number of requests, when you get to a place where registrars are automatically telling you, "No, no, no," sometimes it's a little futile to continue asking for the information over and over again. Not all registrars are like that, but there are certainly some who don't even provide a response, they'll give you the information. You shouldn't read into the fact that you're not getting the requests at the volume that you had prior to GDPR as an indication that there's no demand.

GINA BARTLETT: Thanks, Margie. Mark Sv.?

MARK SVANCAREK: Yes, similar comment about the volume. Our digital crimes people and our threat intelligence people, they're just sucking up their

---

pain right now and waiting for idiots like me to try to work on policy to get them access again. It's just like, "Well, we'll just keep working with the public data. It's impacting the efficacy of our investigation, but at some point there'll be a system where we can begin to make volume requests again." And so, they've been holding off on that. Actually, I'd be happy to discuss what I think our likely volumes would be with GoDaddy, if that were helpful in any way. Thanks.

ALAN GREENBERG:

James's comment reminded me of an old story about when they were trying to decide whether to build Brooklyn Bridge in New York, and someone suggested putting a rowboat in the middle of the river to see how much traffic there was. That's not the way to gauge something that's going to use a completely different mechanism, as Mark says.

I think we have, certainly, anecdotal input from law enforcement and cybersecurity people that there really is a need to be able to do relatively high volumes, and not have them turned around in a day, or two days, or three days, but virtually instantaneously. If that's not going to be possible, then, as Mark says, we'll live in a different world, but it's not going to be a nice world. I think we have to look, moving forward, to the future, not what you're seeing today.

HADIA ELMINIAWI:

I would argue that the merit of accreditation is not only with regard to the volume of the data, or the volume of the requests, but is



---

also with regards to the consistency of the answers to these requests.

JAMES BLADEL:

Sure; in the analogy there was a bridge. It was a great bridge, it was free, it was anonymous. Everybody used it to commute, and then somebody, in their wisdom somewhere, tore it down. Now, we're trying to decide, do we need a tunnel, do we need a bridge? I think what I'm saying is, a lot of folks in the interim have decided that they're just going to take another way to work. We don't know what that number is. We don't know if it's an education problem. It's all speculative. We don't know if it was because there are these new barriers in cost and time, and lack of anonymity that have just caused folks to use alternatives. We don't know these things. What we're trying to say is, we're building this system and this solution for a problem that's undefined. That's my point. We do have people around this table who can give us some of those answers.

MILTON MUELLER:

Can I ...?

GINA BARTLETT:

Go ahead, Milton.

MILTON MUELLER:

The proper analogy, James, is not that somebody tore down the bridge, it's that they put up a toll. Now, you have to do a little bit

more to get access to the data, so of course demand is going to be lower than it was when it was free and could be automatically downloaded in bulk. What existed prior to the existing system is not really a good guide to what the volume will be. I'm not saying I know what the volume will be, but I think James has raised a critical question that we need to consider when we're designing this system, which is, what scale are we in fact designing for?

The relevance and importance of WHOIS data, in my opinion, has been grossly exaggerated by many parties, and the fact that people might take a different way to work, or they might pay the toll, we're going to have a lot fewer requests for that data and uses of that data than we've had before. That's an inexorable law of economics. We don't want to design a system that is essentially assuming that we're going to get the same scale and quantity of requests that we've had before, but we don't want to under-design it either, I'll grant you that. Let's just be modest and empirical about what these expectations should be, and not just assume one thing or the other.

GINA BARTLETT:

Okay, Ashley and then Brian, and then I'll try to summarize. Alan G., do you still have your card up? Okay. Ashley, and then Brian, go ahead.

ASHLEY HEINEMAN:

Thank you, and I'll keep it short. Just to be clear, it's speculative on both sides. You're assuming that the volume is going to remain low, so I think we need to be fair to ourselves. To be fair, I think

---

the whole point behind this exercise was to make it easier for the contracted parties, to provide some predictability on your side. If you're now saying that's not helpful, I still think it's worthwhile going through the exercise of documenting the value of this type of an approach. If it's something that you don't think is useful, then okay, but don't make it a reason later that disclosure and access is impossible, because you don't have any predictability and understanding into who the people are requesting the data.

I'm happy to go down that path, but I think it's also advisable, as we're developing policy, we don't take it off the table for future possibilities, assuming that there is a possibility that there will be a higher volume later on. Perhaps we could say, if accreditation is used, you need to take into consideration these types of requirements or high level principles. I don't think we're articulating the design structure necessary to the policy that could be around it.

GINA BARTLETT:

I'll go to Brian and I'll come back to you, James, to reply.

BRIAN KING:

Thanks, Gina. A couple of points coming from an NPC that has quite a bit of data on WHOIS requests, and how those have worked out when GDPR went into effect. I can offer a couple of points. I really like the bridge metaphor, so if I can sit there for one more second? Pretend the bridge is a drawbridge, and 85% of the time you go across that bridge, you fall into the East River, and you don't know whether the bridge is up or down. When we submit

---

---

requests, when our professional brand protection analysts submit requests to registrars for domain names that we've identified as infringing, many of which have infringing associated website content, we're ignored, or we don't get the data 85% of the time. That's a conservative estimate. It can really be a waste of time to submit those.

I think we will find the ultimate volume in the SSAD will be somewhere in between the request volume of today and the unfettered access volume of yesteryear. I think, realistically, we'll find it to be in the middle, but I don't think we can guess or know with certainty what the volume's going to be. We just have to have a system that works.

GINA BARTLETT: Thanks, Brian. James, did you want to reply to some of the comments?

JAMES BLADEL: Yes, just briefly to Ashley. What you described is the accreditation system that I thought we were heading towards when we came here, which has obvious value. What I've heard in the last hour is that we're not sure who's going to accredit, it's going to be multiple entities, we can't put people into groups, we're going to have to review them manually, and it doesn't provide us any shielding from any liability anyway.

So, why build that thing if I can hire 100 temps to review things manually? This is the question I'm putting onto the table. We don't know if we're going to receive ... We used to receive somewhere

around, I don't know, 250 million WHOIS lookups per month, and now we're down into – from law enforcement, I'll tell you, probably, in a busy day – 12. From other folks, it's probably in the hundreds or in the thousands per week.

Why build something that's starting to look like one of Mark's operating systems? Okay? Not joking, but it's like this massive thing that has all these asterisks, all these escape hatches, all these different checks, all these different things that has processes for accreditation, processes for de-accreditation. Meanwhile, on the flipside, the benefits of doing so is we still don't know if the request is valid, we still don't know if we can trust the party. All we've really established is their identity. We still don't do any jurisdiction matching.

Mark, you used a really important word the other day, which is attribution. You said "attributes". "We're not passing through attributes like jurisdiction-matching." So it seems like the answer is, let's just brute force this thing and let it fall down before we try to automate the perfect – we even talked about putting AI into this. Let's try to walk before we run and then fly. That's what I'm getting at. I'm not saying blow the whole thing up, I'm saying we have unsold ourselves on the value of this versus the cost. Not the best way to end this day, sorry, but it is a very strange place that we've arrived at. I came in here just like, "Let's get this done. Accreditation is going to make things operationally a lot easier." But we put so many exceptions into it that I don't know that I believe that anymore.

---

---

JANIS KARKLINS: May I ask to remain technology-neutral even when we're making jokes? We need always to keep that in mind. I think we maybe spent one hour too long discussing this and we over-engineered at least for the moment. I think we need to step back a little bit and let the dust settle down. Equally, I think it's also time to ask whether those team members who put forward and volunteered on this topic would be willing to continue, provide some input further, based on what we heard, and go slightly deeper in the description of the models that are on the table.

I'm looking, Alex, to you, with the question of whether you would be willing to do additional write-ups, one level lower on the model, with the help of Milton and whoever else wants to join the small team? I'm not asking that for tomorrow morning. I am probably asking it for the first meeting after retreat, meaning the week after.

ALEX DEACON: Yes, I'd be happy to do that. Maybe what we could do is put that diagram. We didn't get to it but on the second slide there was my starting of what these things mean, and maybe we could put that up on a Google Doc and start adding to it?

JANIS KARKLINS: Yes, but if I may ask you to take a lead on that?

ALEX DEACON: That's fine, yes.

---

JANIS KARKLINS:

With the help of Milton and anyone else who would like to join. Also, there was a good proposal for groups which are not obvious, which entity could be used for accreditation to provide a vision of what would the ideal accreditation look like? Again, simply that we tease out some grains from this conversation. My suggestion would be, for the moment, to stop talking about accreditation and let our thoughts settle down, and see what comes up from the further write-ups.

I think that staff also could do a little bit of analysis on what has been said, and then put it further in the structures of the papers that we're working on. We will revisit that at the meeting after the retreat. This is an essential part of the exercise but equally important are the issues we have to address, and if I may suggest that tomorrow we would start our conversation talking about building block on purposes, and see what approach we would take. This is an equally essential element for the discussion.

Now, I think that we have to end, right? I was told by staff that a few hours ago the legal advice from Bird & Bird to questions that have been asked by the Legal Committee have arrived, and as I'm speaking now these answers should fall into your mailboxes. I would like to ask you not to drink too much wine tonight, and to save some money for ICANN, but more importantly that you still have the ability to read that document and be prepared for tomorrow's conversation on legal issues. For the moment, I cannot tell you exactly when that might be, but we will have an initial review of the answers most likely in the afternoon. You need to give time to read and digest the answers. I think that would conclude our meeting today. This is not what I expected.

**[END OF TRANSCRIPTION]**