ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2 LA F2F Day 2-AM
Tuesday, 10 September 2019 at 15:30 UTC

eNote: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
Attendance and recordings of the call are posted on agenda wiki page:
https://community.icann.org/x/6oECBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

GINA BARTLETT: I think we're missing our Board members, but they'll probably get here soon. I think – is Georgios here? I hope everyone had a good dinner and a nice evening. Yesterday, we had these presentations, and the takeaway is that you all have agreed you're going to keep going and develop your policy recommendations and the structures that you'd like to see put forth.

On the accreditation, I know we spent quite a bit of time on that. I'm not going to try to recap all of the discussion, but what we did agree to – Alex Deacon offered to lead on that – is that he will modify the model that he proposed, work with Milton to integrate some of his thoughts, and invite others to contribute on a proposal for the accreditation that will come to a subsequent EPDP team call.

Today what we're going to do is go to a couple different issues and keep having this dialogue that will then inform the draft 1.0. So staff are listening and are going to help frame questions for

you to have conversation. Then we'll document that and bring it back to you in the form of the next version of the draft.

What we thought we would do is start Building Block B on purposes or lawful basis and then have a high-level conversation on Building Block N on financial sustainability. What we're thinking there is a high-level principle conversation, like how you would like to see that take shape. After lunch, we're going to go into the legal memo. Do we have them all now, Caitlin, or are we still waiting for one?

Okay. We're still waiting for one, but there are pretty extensive memos, so we really urge everyone to read that over on the break and at lunch. Leon has offered, as the Chair of the Legal Sub-Committee, to walk us through the highlights.

At the end of the day, after probably the break in the afternoon, we want to talk about the balancing test – where does that occur, how does that take place – and really think that through somewhat.

So that's our proposal for the day. It's ambitious and interesting. Any concerns about at least attempting to tackle that?

Great. Any opening remarks from Janis?

JANIS KARKLINS: Good morning. When we're looking to the hamburger model, one of the building blocks from the demand side is how to bring in the lawful basis in the discussion and how to operationalize the notion of the lawful basis. We saw how difficult this conversation was when we went through all the use cases. Therefore, we discussed

what would be the best way and came to an idea that Marika will maybe outline for our consideration. Again, this is just to try in the most rational plan to bring the lawful basis in a conversation and in this flow chat.

With this, I will invite now Marika to outline this idea.

MARIKA KONINGS: Thanks, Janis. Basically, the part in the zero draft that you're currently looking at is the one focused on purposes. I think we struggled with that already a couple of times in the conversation because I think we're still in the mode of the purposes as we discussed them in Phase 1, while I think here we're looking at the purpose probably with a small "p" and the reasons for why a requester may be requesting data.

However, going, I think, through the use cases, we've seen that there probably is a wide variety of reasons for why someone may want to request data. It may not necessarily be possible for the group to come up with a finite list. There may not be a use in that, either.

But at the same time, it seems that what is a determining factor for how requests are treated is the lawful basis that is identified. As Janis said, one idea or approach could be that, instead of trying to come up with this long list of reasons for why someone may request data and then try to predict what the steps are or what information would need to be provided, would it make more sense to look at this from the perspective of lawful basis?

Say, if someone comes – again, I don't think we'll go into here trying to establish whether someone actually has that lawful basis because I know that's also a point of contention and I think where advice has been requested. Let's say someone comes in and says, "I have a lawful basis: 61D," and that is confirmed separately, maybe through an accreditation or whatever kind of mechanism is chosen. That then automatically triggers a number of preset steps that need to be met, information that needs to be provided, the response time that's associated with that, and information that's typically disclosed. We're just wondering if that might be a way of trying to come up with a predictable way in which requests are dealt with and set clear the requirements and expectations both from the requester side as well as the entity disclosing the data.

So I think that that's one aspect of it. I think several of you pointed out – because really what we put into this section was very high-level. we basically took this from the categories that were identified for the use cases. That definitely was never discussed with a purpose in mind. So this was really a starting point, and I think several pointed out in your comments that that might not necessarily work. I think there were some suggestions here for how that could be potentially rephrased.

But another part of this – my suggestion would be that we probably treat that as two different parts – is of course the big "P" purpose: conversation around Purpose 2. That's also part of this charter question. I think, as you know, the group did define a Purpose 2 in Phase 1 of its work that was not adopted by the ICANN Board. It was already recognized, I think, by this group as

well that that required further work. I think it was referred to as a placeholder in Phase 1.

So at some point – again, it's probably for you to consider what that point is; I'm not sure if that's today – you'll need to discuss if and whether that Purpose 2 is needed and, if so, what that would need to look like. I know that the European Commission has provided some input as well in response to the public comment period that occurred before Board consideration, so there is some input already there. But, again, that's another part of this conversation around purposes.

But I think, for today, we want to maybe first focus on that first question: would it make sense, would it be helpful, to look at this from the perspective of lawful basis and use the lawful basis as a way to map out what would happen if a request comes in [inaudible] and maybe 1A to E would be fairly similarly, and the big one is F – how that would be dealt with, especially the balancing test, which I think we already have as well on the agenda for this afternoon.

So I hope that makes a bit clear what we've been thinking about or brainstorming. Again, it's just an idea to put on the table and see if that could potentially work and facilitate some of the thinking and going through the steps that the group will need to think about.

JANIS KARKLINS: Thank you, Marika. As Marika said, the alternative would be to try to establish a list of most probably cases and then try to associate

with that list of most probable cases possible actions on how to address the issue of purpose. So the proposed idea is simply neater, and, of course, the big issue is we need to assume that the declared purpose is effective. If that's so, then we go through those suggested steps. So that's the idea for conversation.

Thomas was first and then Marc.

THOMAS RICKERT: Thanks very much, Janis. Good morning, everybody. I'm a bit torn on this issue for the following reasons. I think there is a certain beauty in coming up with a policy that is abstract and general and that is for the future crew and is able to cover all sorts of scenarios.

But the issue is that GDPR doesn't [work that way]. Another issue is that I think our group is likely not ready to accept that because what it basically would mean is that, during the implementation of the policy, new use case scenarios of disclosure scenarios would be worked on and that the community or in particular contracted parties would not be involved with that process. So they would putting themselves at the face of some third party.

The question is, I guess to the contracted parties, whether they would be happy with such an approach. So you're giving up a certain amount of control over how the processing is going to take place, whether it's automatic or semi-automatic or entirely manual.

The other thing is, maybe for those who have been following the genesis of European data protection laws, one of the big issues in the pre-GDPR days was that people would, let's say, write up

records of processing activities and then would put them in the drawer and never touch them again. So they were static documents that would be outdated at some point. Therefore, there's a requirement in the GDPR that you constantly revisit your processes and adapt them to current development, to changes in the organization setup, and to the handling of what you're doing: an update of the legislation or updates in case law.

So I think we need to be prepared, and I think some of you will see this as a threat: that we might need a standing committee after this EPDP to revisit this document and keep it fresh. Therefore, my original idea was that we try to come up with a policy that is abstract and general to set out the basic cornerstones of what we're trying to achieve but then we would maybe have as appendix concrete scenarios, including the legal rationale that makes those cases robust and that we would evolve those over time and add to that over time.

So I leave that for you to decide. I think there's a certain risk if we try to play it abstract general and opposite to individual and concrete. But I think that probably the acceptance and the transparency on what we're doing is increased if we keep both of the documents and not only use the use cases for the stated purposes. But I do agree that, in terms of mythology, there's a lot of beauty going through the legal bases rather than starting with user groups or other [inaudible].

JANIS KARKLINS: Thank you. Marc is next, followed by Georgios.

UNIDENTIFIED SPEAKER: [inaudible]

JANIS KARKLINS: Yeah. No, Marc is next.

MARC ANDERSON: Thank you, Janis. Good morning, everyone. Thomas makes a lot of good points that maybe give me pause a little bit. I raised my hand really to agree with what Marika said. Matt, Alan, and I have been having some conversations along similar lines that we were thinking and talking about potentially proposing that we focus on looking at the legal bases and what the policy recommendations needed for disclosure of non-public registration data around each of the different legal bases, not dissimilar to what Marika just proposed. I think we were of independently thinking along similar lines and thinking that that made sense as a way forward. As Marika pointed out, it's an impossible task to try and look at every single use case and account for every single possible reason why somebody might look for access to that data. So maybe shifting our focus a little bit to look at the legal bases I think makes sense.

I think Thomas gave us some real good food for thought. I think it would behoove us to listen to what he said and incorporate that into our deliberations.

Long story short, I think we're generally supportive of what Marika suggested. I think that's a good strategy.

JANIS KARKLINS: Thank you. Georgios, followed by Stephanie.

GEORGIOS TSELENTIS: Georgios Tselentis from the GAC. Good morning, everybody. Two things. The first one is, when we started these discussions, I think already in Marrakech, we tried to finalize that the legal bases are related to [one-to-one] processing activities. So we have to keep this in mind because already yesterday we started growing debates about 61F without being clear about what processing activity we're talking about. So I want to make this again very clear. When we talk about legal bases, we have to match them one-to-one with processing activities and this we have to be consistent with. In order not to put the cart before the horse, we have first to see exactly what processing activity we are talking about.

Now, to the proposal of Thomas, I'm a bit torn. I understand where he's coming from and that he wants to make a sort of bulletproof policy that [inaudible] also changes in the future. But I think we are now in the stage that we have first to define a solid framework for what we have now and all the cases we can identify now. Then we can think in then future how this will be taken into consideration, how we can update the policy.

So my proposal would be let's take things in order and try first, as I said, to identify the right processing activities, get agreement on those according to a model that we will be hamburger or whatever, and put the legal basis for those processing activities.

Otherwise, I think we are stretching ourselves on too many fronts. That's why this group, I think, doesn't have the [face] that it could have for a [inaudible]. Thanks.

JANIS KARKLINS: I'm not sure, Georgios, that I understood what you're trying to say. So what is the process? The request is filed to access non-public registration data for a certain purpose. We're saying that each requester needs to identity him or herself what is the legal basis he thinks he acts on by putting the request in. Then we assess whether that is appropriate – this purpose or legal basis – and, if it is, then we ask data registries/registrars to disclose the non-public data and provide that to the requester. So that's a simplified logic of what we're trying to achieve.

Now, we're talking about if the requester suggested … I think my action falls under 61E, for instance. And we say, "Yes, it does." Then we define that these are steps we need to take in order to get this information to the requester.

THOMAS RICKERT: If I can give you the example—

JANIS KARKLINS: Yeah, please. Just to clarify.

THOMAS RICKERT: If the processing activity we are talking about is, as we did in phase 1, about collection, we have a legal basis for collection.

That's a concrete processing activity. If we are talking about a processing activity, for example, that needs to, in the disclosure to use personal data for the third party, do an authorization, that's another processing activity. For this processing activity, you need again a need legal basis to do so if you use private data. This is what I mean every time.

So each step in the model has a process activity that needs to process personal data. We need to [inaudible] specific legal ways. This is what we said also in Marrakech when we tried to say that each part has to have a [inaudible].

MARIKA KONINGS: Just to respond. I think what we're trying to say – at least I hope that the group understands – is that, indeed, you need a lawful basis for every processing activity. But I think what we're saying here is that, when the requester asks for the disclosure, they will identify a lawful basis that they believe they have to get the disclosure. That is what triggers certain steps. In the rest of the process, that may not be relevant anymore. They still need that lawful basis and they may still have certain requirements, but at least what I think we're trying to say is that, at least for the first step, we look at that the lawful basis identified what requirements or what steps it triggers in the process.

I see …

ALLAN WOODS: I slightly disagree. We're on the right track, absolutely, but we must remember that is not the requester who states the legal

basis. They don't really have a place to tell us what, as a controller, our processing basis will be. So it's up to the controller ultimately. This is probably getting to the core of your point: trying to figure out the roles and responsibilities of us at a particular time in the process of the disclosure. We are the ones that will decide, based on the legitimate interests that are displayed or the request that is displayed to us, what is the legal basis that we will then be processing under.

So it's the other way around. If they just say, "This is my request," then it's up to us to process that and say, "Can we disclose this data, and under what legal basis should we do that?" It's not as straightforward, but I definitely think it's the way to go: we should have a [inaudible] of legal bases under which we can, and each one has a separate process that we will go through.

MARIKA KONINGS: But if I can just ask a clarifying question, you do expect the requester to identify why they believe you should apply a certain lawful basis because they fall in a certain bucket. I'm trying to understand because, if we go down the path of identifying the lawful basis, for this to work, to identify which process we need to go to would be at the requester's side. They would need to identify. "I think it's this. So that's why I'm following this." Then, of course, you as a controller or whoever's disclosing can still say, "I don't think that's right. You actually need to follow this process. So go and fill out these steps."

So I'm just trying to understand, if we go down this path, how that would work in practice. Does that make sense?

ALLAN WOODS: Yeah. You're right. It would be helpful from the frontloading aspect of that. But ultimately it is a wrong expectation on the requester. It is for us as controllers to decide at the end of the day. But if they can say, "We think that it's under this," we can obviously, as you said, go, "No, you're absolutely wrong. It's the other way." We should not be in any way led by what they suggest our legal basis should be. It is us at the end of the day that will decide it.

JANIS KARKLINS: I think that no one questions the legitimate right of the controller to make necessary decisions and use the necessary legal basis to disclose information. But I thought we agreed a while ago, doing these use cases that a requester also needs to state what the requester things is the purpose for the request.

ALLAN WOODS: If I can redirect and probably speak through Chris's brain at the moment, in Chris's LEA example, his legal basis would not be based on anything to do with the GDPR. It would be based on his power under U.K. law enforcement authority. So that's his legal basis. It's not GDPR. Our legal basis corresponding, if I was a U.K. authority, would be 61C. So his legal basis is not going to help me accept to identify that it is a legal basis for me.

JANIS KARKLINS: Okay. Stephanie, please. Help us out, please.

STEPHANIE PERRIN: I think this is a really good conversation because I've been racking my brains about why we failed to make progress on … We look at it through one analytical frame. Then we look at it from another analytical frame. What happens between a disclosure and a collection isn't the same. It isn't like an engineering thing where it's on, off, on, off. He has to figure out a legitimate reason to disclose. I'm not using the correct language here. He has to figure out whether has liability in the disclosure. He will demand a set of facts to verify the particular grounds under which he discloses.

What the other guy does when they get it – that speaks to Thomas's point – is that you have to continue to update your procedures because, as case law comes in and you discover you've been disclosing under a ground that has now been thrown out by a court because in fact they didn't have the right to gather the data for the purpose that they told you, then that update – the template that you have that you cross-examined them on when they request the data … So this requires a lot of lateral thinking here on how you actual put your parameters.

Not to continue to beat a dead horse here, but if you don't know who the controller is and you don't know what your privacy risks are because you haven't done a privacy risk assessment, you don't have the kind of facts that we need to negotiate this very difficult disclosure collection semi-permeable membrane that we're trying to construct in this machine. This will require a lot of templates that the controller has to develop based on feedback that they're getting.

So I think legal basis is, on the one hand, as someone said, and on the other hand because you need facts in order to determine whether you got the legal basis. So the use cases are useful. I'm just worried myself – you probably heard me complaining about it – that, when we started going to use cases, that got us into the camp of what we're looking at is only from a user group perspective as if their rationale for gathering was the same as [use] rationale for disclosing. Do you follow?

So I think we have to [inaudible], have some legal basis, have some illustrations from the use cases. If we don't do that to the templates and the facts, we won't be able to verify our high-level assumptions. I'm very uncomfortable going with high-level assumptions because [inaudible] we don't know whether they're true. But we may be saying, "Oh, yeah. [inaudible] won't work." Well, in fact, it won't. Thanks. I hope that helps.

JANIS KARKLINS: Margie?

MARGIE MILAM: I think I'm leaning towards the approach that Thomas has suggested. I see problems with this approach because we're writing a global policy. We're not writing a policy specific to GDPR. It has to comply with GDPR, but what happens when we have other laws with other bases that we have to somehow accommodate? I think, if we go back to the purposes discussion, there's probably a better place to have a global policy.

When I look at from the perspective of the registrant, I don't think the registrant is going to understand that this processing has happened, what this all means. You're basically asking both the registrant and the requester to really understand the depth of the different bases under GDPR. I just don't see that as being feasible.

So I worry about not giving enough information to the registrant. I worry about introducing confusion to the requesters. So I'm really having a hard time thinking this approach will work.

I know we have to have legal bases, and I'm not suggesting that we don't have to answer those questions. But I don't think that means at the expense of reducing the specificity [inaudible] purposes.

Certainly from the Business Constituency perspective, we really want specificity with regards to cyber security issues, brand protection issues – that sort of thing. If we don't have that in the policy, then it creates a lot of ambiguity as to what actually happens in these cases that we've documented in our use cases. We were submitting requests relating to trademark and cyber security, and I just think it makes it a lot less clear to us that we have a path to be able to get our reasonable requests responded to.

JANIS KARKLINS: Alex [inaudible]. Alex, please, go ahead, followed by Alan Woods.

ALEX DEACON: I just wanted to make a quick comment on how this legal basis will be conveyed to a controller, just to follow up on the conversation and the comment that Alan Woods made.

The way I see that is that the requester is going to make a claim as to their legal basis. These claims are going to be conveyed somehow. I think we're assuming it will be RDAP and secured by OpenID Connect or something similar. These claims can be signed, if you will, by an authorization body. We talked about that possibility.

Clearly, when this request is received by a controller, yes, then they have to go through their process of validating the claims, understanding the claims, weighing the claims. Clearly, a claim made by Alex that says, "I'm this," probably has a little less weight than a claim that would say, "Alex has been authenticated and authorized by some accreditation body that has more weights," I would argue.

So I just wanted to make sure that we put this in the context of, I think, where we're ultimately going, which is a method where these requests can be submitted using modern technologies with the added weight, if you will, of potential authorization and accreditation layer on top of it.

I understand that, once you receive it, then you'll do the processing as you describe. I just wanted to put how I see this happening in reality. I don't want to get into a deep dive on the technology. But we should assume that there is going to be these technical methods to convey these claims. The legal basis is one claim. There may be lots of other claims in the request, too, which

I hope will be helpful to the controllers in their determination of how to respond. Thank.

JANIS KARKLINS: Alan, please?

ALLAN WOODS: Yeah, I agree. Obviously, just to respond to Alex, the best possible case scenarios that the [inaudible] by which this will be given to us. We'll be asking all those question upfront in order to help us make that decision in the end and it would [stream] it appropriately. I completely with agree with Alex, but that's more mechanics than how it would look in the situation. So I agree with you on that.

On Margie's point, I think you're probably broadening what our capabilities are too much here because you're saying, "Yes, we are obviously looking" – I always [inaudible] put my hands up. I'm obviously far too GDPR-centric in my approach, but that's because still in my mind that's a high-water mark at the moment and that's the only thing really guiding us. The CCTA is even a few steps below, so GDPR will cover everything under that. We cannot as a policy-making team look and assume what's going to happen in the future. That's why I prefer the concept, although it gives me breakfast regurgitation, of a standing committee of the future, where we would have to go in and say, "Now there has been this modification. There is this new law that comes in. We may need now to update this dynamic process." The EPDP was groundbreaking. The policy that could potentially come from this

could also be groundbreaking because we could be building into it its own self-modifying thing. I don't know. I don't know what to call it.

So I think we have to focus on what we have now as the legal basis and then allow it to grow so that you can, at a particular point in time, do that.

Matt points out to me something. I'm going to be the first person to break the legal mental barrier of the moment. There is one specific one in the legal memo, which says – I'll just read it very quickly for the record – "The safeguard require attestation by the requester that it has a legal basis for the collection of personal data by the SSAD. Our conclusion above is that the DPs will most likely be due to controllers for this processing. Accordingly, the main concern for the DPs (and therefore for us) will be that they, rather than the requester, have a legal basis for the processing. Where multiple different controllers are involved, the challenge is greater."

So we'll start with the legal – yay! – opinion. So they've already pointed out to us that it's going to be very hard for us. But the focus has to be on our … Therefore, I agree, Marika, we should go along this road. So that's my view.

MARIKA KONINGS: Thanks. I think, to Margie's point, because I don't think we're necessarily proposing that the policy recommendations are going to be written that requesters have to identify lawful basis, it's more at least as I viewed it as a tool to map out the process for how

certain requests are dealt with. Then the group can look at how that is then translated in the policy recommendation. I think then it's probably as well where Thomas's point then comes in. Does that provide sufficient predictability and certainty for the different requests that may come in, or do you need to do more and have indeed more use cases or more templates that are provided. I think we're just trying to see if there's a way of trying to approach it that way.

I think that gets us as well into the question of this afternoon because that's probably the one where there may be more variety in what happens with the 61F, as I understand. So I think that's a bit what our thinking was on using that as a concept and not necessarily immediately saying that's the limitation of what we're doing.

[MARGIE MILAM]: If it's a tool for discussion, I don't have a problem with it. But if it leads to where there's no specificity in purposes, I just want to flag that that's the area that causes concern. If, through this process, we end up identifying a list of purposes that can be used for access of the data, then I'm okay with it. But that's why I raised the concern. It sounded like we were going to eliminate the concept of purposes. Really what we're doing is just working our way to the place where we'll be more specific.

JANIS KARKLINS: Probably by going this route we also can add additional legal bases if they come in at the later stage.

MARIKA KONINGS: If I can just add one more thing, I think at some point we may as well need some scenarios, especially in 61A. What does that look like from the contracted party perspective? What types of request would they envision falling in that category? That may help as well with making it more concrete and making sure that variety of requests are [inaudible].

JANIS KARKLINS: Stephanie?

STEPHANIE PERRIN: Thanks very much. I don't want to over-complexify this, but as we discuss this whole semi-permeable membrane and the purposes, I think one of the problems that we are fraught with here at ICANN as a multi-stakeholder organization is that we are doing this [inaudible] here, as they say in French, in our multi-stakeholder roles. We assume that the purposes of all the different stakeholders are therefore ICANN's purposes, and they're not. Nothing is more acute than that difference when you're in a disclosure collection situation where the grounds for disclosure have nothing to do with the other party's purpose for collection, except insofar as they provide you evidence for a permissible disclosure under your rule.

But by continuing to talk about purposes of user groups for their generalized collection, that really confuses our discussion as a group. We need to know: controller here – that's why I don't like the hamburger; it's merging it all together – controller over here,

controller over here. My Save the Turtles group has enough evidence to provide a legal basis for disclosure. It has nothing to do with the LEAs, really, because it's administrative law. It's separate. These things are disparate [inaudible] LEA. They're [great] entities with separate data processing rationales. I think we're merging because of the MS model. The first stakeholder at the table was WIPO. WIPO's purposes are not ours. Thanks.

MARIKA KONINGS: Indeed, if there's agreement to go down that road at least as a starting point, one thing staff could do – I see it almost as a table – is we list the lawful bases and then the columns indicate what information would be required to be provided/what is the expected response time. Then we can maybe see if that differs depending on which lawful basis is used to disclose, or if there's actually commonality across all of those. Again, where there's commonality, you have probably then one policy recommendation that may address that.

But there may then be cases where it differs depending on which lawful basis is applicable. Again, I think a big chunk as well of that work will probably in the discussion this afternoon in relation to the balancing test and what that looks like.

[STEPHANIE PERRIN]: So should turn to Purpose 2 next and talk a little bit about how Purpose 2 is managed? Or you [inaudible]?

JANIS KARKLINS: No. I'm thinking. Margie mentioned that we should also constitute the list of purposes for submitting requests by requesters. So wouldn't this be a good time now to simply generate those purposes, at least groups of purposes that we know what is the general thinking in that respect? We're talking about IP protection, so that would be one bigger group of purposes to submit requests. We're talking about fighting criminal activities. We were talking about—

UNIDENTIFIED SPEAKER: [inaudible]

JANIS KARKLINS: Oh, yeah. Okay. In that case, I rephrase. Would those five bullet points suffice as a general list for submitting the requests? That's in the document, the zero draft. That was sent around.

Milton, yes?

MARIKA KONINGS: Just to add one clarification or reminder that this list comes from the categorization that a small group – maybe Milton will talk more about that as well – did in grouping the different uses cases together. So this list was not specifically developed as a staring point for purposes. Again, I don't know if we should be starting to use a different term because I don't think we're talking here of purposes with a capital "P" as under GDPR. So I don't if this needs to be called something different. Maybe I'm looking at the experts across the table about what might be appropriate

terminology. Just to provide you that background. This is definitely something that we flagged as maybe needed further work. This list was developed, but it wasn't specifically with this charter question in mind.

JANIS KARKLINS: Milton?

MILTON MUELLER: I'm getting confused. I just want to clear up my confusion. So we have purposes, so-called. We have user groups, and we have legal bases, right? Now, I've never been a fan of user groups. You probably all know that by now. It's infinite and not mutually-exclusive lists. Purposes are a little better, but again there's a lot of overlap in those purposes as we had pointed out.

I agree with Alan Woods' argument that the legal basis will be determined by the controller in its application, but I'm not sure why it is not acceptable for requesters to channel their request with an assertion, unverified and not necessarily accepted, that this is a 61F, this is a 61C. Then, of course, the decision as to whether that applies would be made by the controller. But it seems to me to be much more streamlined and efficient for the requester to make an assertion as to what they're requesting. It's better than purposes and it's better than god forsaken user groups. So that's …

[STEPHANIE PERRIN]: Milton, I think everyone is saying that the requester would provide the assertion of their lawful basis, but the controller would make

the determination of whether or not that is the lawful basis they're going to rely on.

MITLON MUELLER: Okay. So I'm just like two steps behind everybody else.

[STEPHANIE PERRIN]: Because I see everybody is nodding their head.

JANIS KARKLINS: Milton, also I don't think that user groups are part of this conversation. So requests are submitted on an individual basis. User groups are more used for the accreditation purposes if we are going on that path.

Hadia, please, followed by Marc.

HADIA ELIMINIAWI: I do agree with Marika's proposal to have the lawful basis starting point. It does make sense. It's what been determined and set by GDPR.

To Margie's point, I also agree to have a possible list of possible purposes and a possible list of user groups. Maybe what we have on the board now is a list of possible purposes for disclosure. That does not mean that these are the only – well, very much. It might be the only purposes that are available for disclosure, but there might be others that we never thought of or envisioned. So having a list of possible purposes is also essential.

To Georgios' point where he was actually talking about the processing activity and the lawful basis, the processing activities that we are clearly talking about in relation to the standardized access or disclosure model is simply disclosure. So I don't envision any processing activities through this model. No data would be collected through the models, for example. Right? It's a disclosure model, right? That's at least my understanding. So we don't envision other kinds of processing activities happening through the model. Right?

JANIS KARKLINS: Marc, please?

MARC ANDERSON: Thank you, Janis. You've given us lots to think about and I think we're on the right track, but looking around the room, I think maybe we could use a quick ten-minute break to caucus with our groups. I think it's been a great start to the conversation. I think we're on the right track here, but maybe a quick break for everybody to caucus would be a good use of time here.

JANIS KARKLINS: Okay. I will take – these are new flags? Let's take Georgios and then Stephanie.

UNIDENTIFIED FEMALE: I think we'll take a caucus.

STEPHANIE PERRIN: I hate to be difficult, but in that list, which we're describing as legitimate interests, the last one – the registered name holder consent – is not a legitimate interest. That's a lawful basis for disclosure. If you are the disclosing party, your next question, reaching to my template, is, "Show me the collection instruments on which you got that consent. If I don't like it, you're not getting it." So I think we have to be analytically clear as we follow these from basic concept down to fact. That one doesn't belong on that list.

JANIS KARKLINS: Thank you for flagging that. Georgios, please?

GEORGIOS TSELENTIS: Just to answer to Hadia, when we say "disclose" or we have several – according to the discussion yesterday, we have several items [inaudible]. We had identification, authentication, authorization, and transfer. All these are processing activities. We have to find out under which legal basis that we are talking about that we have to process the personal data under. This is what I'm talking about.

So by saying that disclosure has one legal basis, we have to see every processing of personal data, how it is managed, under which legal basis we do when we process this data. This is what I meant [from my original intervention].

JANIS KARKLINS: So then the question/clarification for you is, can we think that there might be different lawful bases dealing with the one request going through each of the steps?

GEORGIOS TSELENTIS: It just depends on the scenario of the model. I think we are in this Catch-22 where the model … If we haven't decided in the model how, for example, the data flows go, then we might not know the exact legal basis that we are processing these data under. That's a Catch-22 that [inaudible].

[MARGIE MILAM]: I think we're going to take a caucus. There was a request for a ten-minute caucus. I think, on Building Block B, if I understand where we're at – I may not have it quite right, so you can discuss it on your caucus and come back – the concept is that the requester would – I like the word "assert" – the lawful basis for the request. The controller would use lawful basis to determine whether or not they are going to proceed. We would use this for the policy purpose of looking at the lawful bases in order to identify the process – so the response time or other triggers or steps in the process – and staff would flesh that out. Then, where you saw commonality across the different legal bases, that might pull out some general policy recommendations.

But what we're also hearing is that there is an interest in continuing to identify a possible list of purposes – I think small "p" purposes, correct? – and it may or may not be complete. I think then question is where to capture that. It is part of this building

block or in an annex to the policy? I've heard a couple different options.

I think that's where we're at right now: to take that to the caucus and massage that and think about it a little bit more.

JANIS KARKLINS: So shall we say 15 minutes for conversation?

I was using this 15/20 minutes to understand what we're talking about. There are many ifs in this scenario, but the reality is what we want to tease out from the group is how to proceed with the description of purposes and the lawful basis for disclosure of information in the policy.

We can split actions of disclosure into three steps from the processing point of view. The first action is to make a decision on whether to disclose information or not. So that would be the first processing action. If the decision is no, then the game is over. If the decision is yes, then the next action would be to decide on which data elements to disclose, pull them out from the database, and form a data file. So that would be the second processing action. The third processing action would be to transfer that data file somewhere. So these would be three physical actions. Each of those physical actions need to have its own lawful basis as is requested by GDPR. So that is what we're in reality talking about.

Now I would like to see how much wiser we are after discussing through all the elements of this morning's conversation. Who will start?

Marc?

MARC ANDERSON: Thanks, Janis. I feel like, since I suggested the caucus there, I have to jump in. So I'll start. Registries and registrars – we went outside and talked through it. We think there is merit in going through the steps you laid out from a legal basis perspective. We think probably 61C and 61F is where most of the action is. Obviously that's where we'll spend most of our time – focusing on those – but I think it's probably worth looking at each of the possible lawful bases under GDPR. From a policy perspective, we'll go through each one and see what possible policy recommendations would we need for each of those lawful bases.

We realized this may not be a silver bullet. I think we have to be willing to adapt and change if this doesn't work. If we're not taking into account some purposes that are important, we can obviously shift. But we think this is a good path for us to move forward with. So we'd like to see a conversation abut each of the different lawful bases and what would be policy recommendations that we would want to consider for each of those.

JANIS KARKLINS: Thank you, Marc. Chris?

CHRIS LEWIS-EVANS: Thanks. Slightly separate. We had a little bit of discussion around the small "p" problem. One of the suggestions we'd maybe like to make is to change all that language so it reads – sorry, I'm just

getting the actual language – “A function of processing.” So it could read, “Identity at a minimum. Identify its function of processing personal data.” So it gets away from the whole legitimate interest purposes and problems. Really what we’re saying is, what is the requester’s reason for processing information? [So it’s] a function of processing, to be able to assess—

UNIDENTIFIED FEMALE: Can you repeat it one more time, Chris, what you’re suggesting [inaudible]?

CHRIS LEWIS-EVANS: How about I type it into the chat?

UNIDENTIFIED FEMALE: Good. Thanks.

JANIS KARKLINS: Anyone else?

Alan?

ALLAN WOODS: One of the things that occurred to me as well is that all these five are not exhaustive. So we would need a sixth, and the sixth is literally Other, as in anything that’s not under this. So why go through each one of these when, if we just focus on the other, it

will cover everything? I think that's the way we actually need to proceed. That's why I [inaudible] legal basis. I'm trying to be a reformed person. I know, Marc, that you were saying, "Under the GDPR." Why don't we just say "legal bases"? We all know in the back of our head we're talking about 61s. But for policy purposes, as Matt and James put into the chat earlier, perhaps we should talk about them as legal bases as concepts as opposed to that we know they're linked to the GDPR. But for the policy purpose, let's make it agnostic as to the GDPR. Oh, gosh. Such a burden off me now.

JANIS KARKLINS: Thank you. Hadia, please?

HADIA ELIMINIAWI: I would like to go back to Georgios's [inaudible] intervention with regard to the processing activities. I know that you have put on the board certain bullet points. First we have – we're talking again about the model – a decision for disclosure. That would require a lawful basis. Depending on what Marika said, our starting point is the lawful basis. So we'll look at the lawful basis. Then, again, the decision for disclosure – that's confusing for me. Is it the contracted parties? Would it be the same if the decision is made by another entity? I don't know. But let's say the decision – yeah, of course. I think it would. Definitely it would. So the decision for disclosure would require a lawful basis.

Then, after that decision has been made, whether yes or no, then the second activity – which data elements to disclose – would essentially rely on the reason for disclosure, the purpose.

Then you have #3, which is the transfer of data. That would require another lawful basis because, if the disclosure of data is done from the contracted parties, for example, to ICANN, who will eventually disclose it to the requester, then the contracted parties would have to have a lawful basis to disclose the data, to transfer the data, to ICANN. So that would require a different lawful basis than the lawful basis they had essentially made or taken into consideration when making the decision.

So I think, again, that relying on the lawful basis is a good way forward. Again, I agree with Chris' suggestion on the reasons for disclosure or access. We should mention some.

Also, to Margie's point in the beginning, where she was actually also saying that it's good to identify user groups, yes, I do agree with that because some user – but that should be a guiding thing but not like those are the user groups are going to use the system. Thank you.

JANIS KARKLINS: Thank you. Marc?

MARC ANDERSON: Thanks, Janis. I just want to respond real quickly to one of the things that Hadia said. In the process flow, you described a model where the contracted parties would flow the data through ICANN.

HADIA ELMINIAWI: Maybe. Maybe not.

MARC ANDERSON: Okay. Yeah, that was the point I wanted to make: that would be one possible model. We could proposal a model where ICANN is the central clearinghouse for all the data. But if we look at what the TSG report proposes, for example, ICANN doesn't possess the data at all. In the TSG model, they're taking on the decision-making process, but the data doesn't actually flow through ICANN. The requester still gets the data from the contracted party who controls the data.

So just responding to that, these are decisions that we have not made. These are some of the fundamentals about, is it going to be centralized? Decentralized? Will it be a single clearinghouse for the data? Would it be – Mark's not here – a hub-and-spoke model, which I think we've all heard him talk about?

So I just wanted to jump in and make that clarification. We could propose a model where ICANN – I'm making Trang nervous over there – possesses all the data, but I don't think that's really— don't worry, I'm not— a model we seriously talked about. So that was just a clarification.

HADIA ELMINIAWI: It was just an illustrative example that the lawful basis could change. It's just for illustrative reasons, not [specifics].

JANIS KARKLINS: I think we have reached for the moment the limits of this conversation. I would say we need probably now to digest a little bit and start with maybe doing the first write-up and then circulate to the group for further consideration.

Stephanie, your flag was up.

STEPHANIE PERRIN: Thanks very much. Not to nitpick, but from a security perspective, you wouldn't want ICANN to be holding the data. You would want it to remain in situ. The actual "ownership" of the data is irrelevant in terms of whether ICANN is the controller. To me, the interesting question is, where does that controllership point kick in? In the management of this particular EPDP? In the passage of our policy by the Board? That makes them the controller, right? Particularly if they're going to send GDD in to bust the contracted parties if they fail to respond, that's an enforcement action that reads controllership.

So let's be clear about this. Where the data is is irrelevant. It's who calls the shots that's relevant.

JANIS KARKLINS: We will be talking where disclosure decisions could be made in the afternoon, after reviewing the legal memos. I hope that we will get at least a sense of the room on this very topic later today.

Dan?

DAN HALLORAN: Thank you, Janis. My reflection of the TSG report is a little bit rusty now. It's been a few months. It's a little bit different. My recollection of the TSG report and their models was a little different. I thought the request would come in through a central gateway, and then the gateway would give response back to the requester, and then they had several different models. The gateway is not necessarily the same entity as the authorizer. The authorizer would be making those decisions about who gets what data so that neither of those need to be ICANN org, they could both be ICANN org , and either could be ICANN org. They separated those decisions out.

I think, in all their models, the data would come in from the contracted parties – the full set of data. The central gateway would strip out what wasn't need for the policy to go to that requester and send that and then flush the data immediately. So no data ever sits either before or after at the central gateway. It just temporarily flows through their out to the requester. Thank you.

JANIS KARKLINS: Thank you for this clarification. As I said, maybe we ask staff to do the write-up and then send it out for consideration. We will address whatever comes out from that write-up at one of our next meetings.

We have about two hours. Maybe we can use that time to address two things. One, very, very quickly, is going just to collect views at the moment on what we now do with Purpose 2, which was

rejected by the Board. As Marika explained to me, we need to make a decision. The decision is what our options may be. Maybe, Marika, you can suggest what our options are that we have to contemplate in relation to the outstanding question of Purpose 2.

UNIDENTIFIED SPEAKER: [inaudible]

JANIS KARKLINS: Marc?

MARC ANDERSON: Sorry. Quick question before we move on. Apologies for this. Chris, you suggested updated text. Sorry, I got a little bit lost. I'm not sure what you're suggesting the updated text to, so could you – sorry, I couldn't quite follow along – clarify that?

CHRIS LEWIS-EVANS: I posted it in the chat.

MARC ANDERSON: Yeah. You're suggesting new text. To what?

CHRIS LEWIS-EVANS: Ah, okay. Sorry. To the language that's on the screen, just below the comment box. So, "The EPDP team recommends that requesters must be able to …"

MARC ANDERSON: Thank you.

JANIS KARKLINS: Just for our better understanding, what are our option that we have with Purpose 2?

MARIKA KONINGS: Thanks, Janis. As a refresher, I think everyone may remember that the group spent quite a substantial amount of time in Phase 1 on working on a purpose that would factor in or allow the disclosure of data to third parties. I think there was a hard-fought compromise that the group came up with. I recall that some were very firm that that was necessary and required in order to be able to develop a model that we're discussing now, while I think others were of the view that you don't need a purpose to be able to do that; it's already something that is expected and can be done; you don't need a big "P" purpose statement for that.

But in the end, I think the group came to a compromise to include it in its recommendations. A lot of work was done on the language. But then, when it went up to the Board and before the Board considered it, there's always a public comment requested or input on the recommendations that it's considering. I think one of the inputs received was from the European Commission with some concerns on the way that the purpose was phrased. I think the Board took that on board and decided to not adopt that recommendation.

Having said that, I think group recognized already in Phase 1 that it would need to review that purpose statement in the context of the work being undertaken here and see how that would need to be modified. But, as I said, the Board didn't adopt it. I think there's an expectation as well from the Council. The Council knows it's already enforced within the mandate of the group to look at that again.

So I think the question for the group is, is it still the belief that a big "P" purpose is necessary to be able to do everything we do here? If everything here is defined, it that impossible without having that purpose statement? If it is, obviously it will require work. I think then the subsequent question is, when we would be the appropriate moment to have that conversation? Is it something that needs to happen sooner rather than later? Is it something that would need to happen at the end once you're completely clear on your whole model? Or is the view that, once you've agreed on all this and outlined and everything and written everything up, you don't really need that purpose (capital "P") statement because you've actually documented everything that is needed in your recommendations?

So I think that's the questions. I don't think we want to go here into, let's look at it and rephrase it and change it again. I think it's really more to get a sense from the group of what you think is needed or required. That's for the planning of our work. We can factor in where that conversation should be had if it is deemed necessary and align the work plan accordingly.

JANIS KARKLINS: Thank you, Marika. The reactions now. Leon is first. Leon, go ahead.

LEON SANCHEZ: Than you so much, Janis. Can you hear me? Yeah? No? Not really, right?

JANIS KARKLINS: You need to go closer to the microphone.

LEON SANCHEZ: Maybe here?

JANIS KARKLINS: Yeah. Lick the microphone and then we will hear it.

LEON SANCHEZ: Just to remind us all that the recommendation wasn't really rejected but just not yet accepted as it needs to go through further discussion with the GNSO Council. So just to make that clarification.

JANIS KARKLINS: Thank you. Milton was second and then Thomas.

MILTON MUELLER: I think it's obvious from the hours and hours of discussions that we've had about SSAD that we don't need Purpose 2, that its

status is pretty much irrelevant to our discussions. The people who are requesting data, requesting disclosure, would have a legal basis for it or they would not. Whether ICANN has a purpose for disclosing data is not really relevant to that. There's a legal basis for it, and that's what is driving the requests and the structure of our process for giving out the data.

So it's not like at any point in these discussions – we've had intense discussions about accreditation, about who makes the decision, about what is a proper legal basis to apply to use cases – has somebody jumped up and said, "You know, if we don't have Purpose 2, none of this can happen." That has never happened. So I think we could save ourselves a lot of time and trouble by saying we don't need this.

JANIS KARKLINS: Thank you. Thomas?

THOMAS RICKERT: Thanks, Janis. I guess there's a political dimension to this and a legal dimension. The reason why I wasn't more outspoken when it came to this purpose during the first phase is because I did recognize that some on our team had the fear that, if we don't explicitly mention this as a catch-all purpose, they would lose something. I think that at this point it's probably still valid.

So I think what we will find is, when we plow through the legal bases, we will come up with a finite catalogue of scenarios in which disclosure can take place and in which disclosure is not

possible. That would potentially render Purpose 2 completely irrelevant for our work because we will have a finite list.

But, as much as I sympathize with the idea of not needing it, it might be politically well-advised to keep that open and see whether there's a need for something that is not covered when we advance our discussions more and whether we need such a catch-all.

The legal implication, though, is that you need to be transparent to data subjects as to what is happening to their data, right? And for certain disclosure scenarios, such as 61C, you don't need to make that disclosure because you're following a legal obligation. For other things, if you want to change directions, there's a more or less complex procedure of changing the purpose of processing. But let's see how much is less. Let's first plow through the legal bases and benefit from the work that we've done so far and see whether there's still the need for such a catch-all, which I think is always a difficult to robustly implement legally if we don't attach it to concrete scenarios.

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

ALAN GREENBERG: Thank you very much. I'm half agreeing with the previous two speakers. I'm not sure we need it. It does [inaudible], but one of the aspects we haven't looked at is that ICANN's mission is relatively wide in terms of preserving the security/stability of the Internet. It's well-acknowledged that we can't do it all ourselves.

So providing the mechanism as an ICANN purpose to make sure that others can do the parts of our job, which we can't do ourselves, I think does have merit.

Now, that may or may not apply to the IP issues. It certainly applies to the cyber security issues where, although we're not doing the work, we don't need the data. It is an ICANN purpose the preserve the security and stability of the Internet. So, from that perspective, I think there is merit to keeping it: to document that the fact, although it is a third party unconnected to us doing the work, it is our purpose.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I agree with Thomas and Alan. I think that the European Commission letter didn't say we didn't need the purpose. It just simply said you're not conflicted with the two purposes. So I think it's a mistake for us not to have a Purpose 2. I think we will get to more specific purposes through this process, but if you think about the timeline, Purpose 2 is part of the Phase 1 implementation, so we need that for Phase 1 implementation by February 28th of next year, when it goes live, or there is on third-party access to policy. That's the one place in the ICANN policy from Phase 1 where it talks about third-party access.

So my suggestion is that we actually make a recommendation to update Purpose 2 to be consistent with what the European Commission said, have that be the placeholder until we finish our

work and we do what we need to be more specific, and then eventually it'll replace it. But to have no Purpose 2 I think is a problem. That's been the position of the BC since even before Phase 1.

JANIS KARKLINS: Thank you, Margie. Marc?

MARC ANDERSON: Thanks, Janis. A quick reaction to Margie. I understand your concern. I don't think not having –ugh, double negative – a Purpose 2 means there's no third-party access. I think there's still the possibility of third-party access without Purpose 2. But I certainly understand your concern there.

Why I raised my hand, though, is because I suspect everybody is aware of the GNSO Council consultation with the Board. That process is going on. I think yesterday the GNSO Council published their letter to the Board. I'll just put an excerpt from that into the Zoom chat for everybody. It's a little bit long, but I think it's important that we understand that Council is expecting the EPDP as part of Phase 2 to consider this and get back to the Board. You can read the text yourself, but their expectations are: "After such consideration, the EPDP should report back to the Council with its updated language."

So obviously we're chartered from the Council. They give us our marching orders. It seems clear to me that we can't ignore Purpose 2. We have to consider it and provide a recommendation back to the Council as part of our Phase 2 deliberations. That's

not to say we couldn't deliberate it and say, "Hey, we all agree that we don't need Purpose 2 for third-party access, and this is why," or we could say, "Hey, we looked at the advice from the Board and we decided here's our updated language." I'm not presupposing what the outcome is, but I think it's clear we have to consider this in Phase 2 and we have to include that in our response back to the Board.

JANIS KARKLINS: Thank you, Marc. Ashley?

ASHLEY HEINEMN: Just to agree with some of the past comments, particularly comments. I think it'd be premature at this point to toss it out. I think, in the context of also, as we're trying to figure out where we're going to align in terms of an actual model, it might helpful even to get some input from ICANN if they need that coverage if they find themselves in a situation where they're responsible for a disclosure type of regime.

That being said, I disagree that – well, let's continue to consider it.

JANIS KARKLINS: Thank you. Mark Sv was next, followed by Stephanie and then Brian.

MARK SVANCAREK: I'm also of the mind that, while we potentially won't need it, that all the bases will be worked out in detail, it would be premature to

remove it in this time. Keeping it as – what was Thomas' phrase? – a fallback or a grab bag or something like that I think is prudent at this time.

JANIS KARKLINS: Thank you. Stephanie?

STEPHANIE PERRIN: Thanks. I just wanted to say that, had we done a privacy risk assessment, we would have identified legal risk, reputational risk, which I think is part of the point that Thomas was trying to make – we need it for transparency purposes to our registrants and for various other reason, but we don't necessarily need it for legal accountability. That's a bright perimeter that I think we want to draw around ICANN's activities. What are they actually accountable for? It gets back this conflation. Picking up on what Alan Greenberg was saying, yes, it's in ICANN's mission, but let's not confuse mission statements with purpose of processing. ICANN is not processing data to a great extent for the security of stability of the Internet. That's part of their mission statement. So you have to be clear.

On the other hand, as Ashley just said, ICANN may have actions where it's releasing data under that. So we kind of need it in there, but, again, we'll find all this out when we do the data analysis of specific processing activities. Thanks.

JANIS KARKLINS: Thank you. Brian?

BRIAN: Thank you. And thanks to Marc, who made the first point I wanted to make about the Council letter. It gives us our marching orders today that EPDP should report back with updated language. I think that – yes. Thanks. Marc made a good point that I wanted to make about the Council saying that we should report back with updated language. So that says that we couldn't toss it out.

Thomas made a good point about transparency. I think if we take back step, a commonsense thing [is that] this is the purpose of the SSAD data. The contracted parties said they don't need it. The purpose says that it's available for the third parties that do. I get the language shouldn't conflate those things, but I'd like to have that commonsense perspective in our heads.

It seems to me that the general consensus is either that we do need to have the Purpose 2 language or that maybe we don't need to have it. But I haven't heard any arguments against having it. So if there's no arguments against having it, let's just do it. Thanks.

JANIS KARKLINS: Thank you. I think that was a useful exchange. Alan, you spoke already, right?

Yeah. So we will revisit this issue at the later stage once we will be having a better idea of how our policy document or policy recommendations look. But obviously we need to respond to the Council's invitation. That is explicit: EPDP should report back to the Council on its updated language. I think the expectations from

the Council are clear. We need to update the language of Recommendation Purpose 2.

Margie?

MARGIE MILAM: With regard to that, I read the Council letter as saying that that comes before our report, that the request has a more immediate timeline to it. So if we could factor that into our work.

MARIKA KONINGS: Margie, at least from understanding of what has been discussed, I think it's the expectation that it's discussed as Phase 2 deliberations. I haven't heard anyone indicate or say that that should be received sooner. Or at least that's what I've understood from the conversations today.

MARGIE MILAM: But what we just read said, "After such consideration, it should report back to Council with its updated language." So that to me sound like a …

MARIKA KONINGS: If you read further up, it refers to the Phase 2 deliberations. Again, maybe it's a point that the group wants to clarify, but that has been my understanding.

MARGIE MILAM: [inaudible]. Right.

JANIS KARKLINS: We will come back to this issue as we progress. Again, for the moment, I would not give any specific timetable. But as we progress, we will always keep in mind the need to look at the language.

Now I would suggest we think about money. It's always good to talk about money. I especially count money in the pocket of a neighbor, not in your own. More seriously, the group identified the financial aspects of the SSAD or functioning of SSAD as one of the priority issues. Here, if we think again in logical terms, there is a cost associated with setting up a system, Including potentially designing automated tools.

UNIDENTIFIED MALE: Thanks, Janis, and I agree. I won't stand in the way of our breaking up into smaller groups. I just wanted to add that there are the initial costs to develop the system, there are the maintenance costs. Hopefully, in that second bucket, we should be thinking that maintenance costs will also include any human costs to check any balancing tests, any audit costs, as well as any costs associated with accreditation, maintaining, checking, verifying credentials, and also possibly revoking or [pressing] appeals. I think we should think of all of that when we think of maintenance, not just paying the electric bill and keeping the phones turned on, but all of the people that will be involved in processing these.

JANIS KARKLINS: Yes. And I think we have the papers that everyone can use, so please, each group, take one paper and bring back in 10-15 minutes a proposal. Thomas.

THOMAS RICKERT: I'm sorry, Janis, I think I'm not clear on what we're tasked with. Are we to discuss general parameters on how things are going to be financed, or are you expecting projections on what the overall costs would be? Are we only talking about the costs for ICANN, or are we also talking about the implementation and onboarding costs for the contracted parties? I'm sorry, I'm a little bit unclear. I think, if I may offer something constructively, in order to get the complete picture we would need both the costs for implementation and maintenance at the ICANN level, as well as the cost for the contracted parties to get on onboarded with this process.

We need the legal risk fund in order to protect ourselves against third-party claims, and then we need to make projections as to what the volumes will be. You have a fixed amount of costs, but then you also have varying costs depending on the overall amount of queries. What we haven't discussed so far is bringing on board technical experts to help us with studies into encryption and pseudonymization, and all of that. I think we haven't done anything about that at the moment. I'm totally lost when it comes to fleshing that out.

JANIS KARKLINS: Look, exactly. This is the reason why we're not setting any specific parameters.

THOMAS RICKERT: Okay, so you want to leave it unclear.

JANIS KARKLINS: Just come up with what you feel is right. You see four bullet points in the zero draft.

UNIDENTIFIED MALE: Janis, I have an even more fundamental question. When we talk about the cost of the system, are we assuming a centralized system? Are assuming that we're building a machine, or a system as envisioned by the TSG? Or are we …?

MARIKA KONINGS: I think we need to take this a level up, because this group is not going to be tasked with calculating the cost and thinking about who is going to pay what. I think we need to take it up a level as the policy principles. Indeed, maybe those differ whether you're looking at a centralized model or a decentralized model, so you can separate it out, but I think it would be helpful if the group thinks about what's currently in the zero draft, which is TBC, and kind of think about what are the kind of recommendations you want to make? I'm more thinking of, "The model should be cost-neutral, or shouldn't bring extra costs to registrants," kind of that level. Some of this will be done in implementation, or needs to provide guidance to the implementation phase how that's then translated. That's at least …

JANIS KARKLINS: No, we do not want numbers, we want policy principles. Who is funding? We heard for instance from business group that requestors may pay for submitting each request. That's one option. Again, I'm not prejudging anything, but just asking to come up with your vision on that. Alan?

ALAN GREENBERG: Thank you. You asked, can we take away the pieces of paper and come back with a model. I think coming back with a model is premature. I think what Marika was talking about is exactly the issue. Come up with a list of the issues we need to consider when coming up with a policy. I think until we've had a discussion of it, I don't think we can come up with a model. I don't understand enough about some of the other people's issues to design a model at this point. Let's focus on, "What are the important things we must consider going forward?"

JANIS KARKLINS: Agreed, and the presentation after will kickstart that debate. That's the beauty of the beast. Stephanie.

STEPHANIE PERRIN: Not to be tedious, but this is basically a regulatory impact assessment that you're talking about, and kind of normal. You assess the impact on all the stakeholders that are impacted by this new policy, and what the trickle-down would be. You don't need number facts yet, but it's going to help you lead to it. If you

have any, they should go on the table. I don't really want to discuss it unless we're going to do it in a properly structured way, as one would do in a regulatory impact assessment. Thanks.

JANIS KARKLINS: Thank you. 15-minute break for group work.

GINA BARTLETT: Okay, I'd like to encourage everyone to get out of their chairs for a couple of minutes and come over, and just look at these sheets, and then in a minute when everybody's done, we'll ask a wrap from each group, to talk us through it. If you could just get up and have a look, and look at everybody's concepts, that would be terrific.

I don't think, during this stage, you guys need to stay in your seats if you want to look, because what we're going to do is … You have a charge to do two things. One is to develop policy principles tied to financial, and then also you have the option of putting things into implementation guidance. That's our charge of this day, to identify the policy principles and/or notes for implementation guidance. The trusty staff will take your insights from this session and write up a proposal to you.

What I'd like to propose is that we just move down the list and hear one to two minutes from each group. I have the Commercial Stakeholder Group, is that what CSG is? Can you just walk us through the highlights or takeaways from your group?

MARK SVANCAREK: Hi. Here are some principles from the Commercial Stakeholder Group. We resisted trying to come up with a definitive list of all the places we're costing. We started down that path, but I think the request was to look at principles and so that's what we did. We really were able to get this down to two basic principles. One of them is, it does seem fair for different types of requestors to contribute differently to the cost-sharing of the system.

There are a few ways that you can slice that. There are certain requestors who have greater volume. There are certain requestors who have different monetary capabilities. An academic researcher might not have as much capability to pay the same for a certain level of request as Microsoft, for instance. Some people will be under legal obligations. Some request types might be more costly. As a principle, we think that cost-sharing, applying it differently in different cases, probably makes a lot of sense. We think that within that principle simply saying there will be a per-request fee, or a per-domain name fee, probably isn't a good choice.

The second principle is that we must not create incentives within the cost-sharing, or disincentives within the system, to prevent cost reductions. If we have a principle that cost will be passed through to the requestor, then there is never any incentive to reduce the costs that are passed through to the requestors. You could just build the crummiest most costly process and then pass it through. We think that, as a principle, that should be disincentivized.

GINA BARTLETT: Sorry, provide for cost reductions where possible? Don't prohibit or disincentivize cost reduction?

MARK SVANCAREK: You don't want to dis-incentivize them. I think there are other people who were saying things like, "Don't make this into a profit center."

GINA BARTLETT: Got it.

MARK SVANCAREK: There is this perception that if are a badly run registrar and you're selling a million domain names for a nickel, and they're generating a huge amount of abuse because of your cost structure, and then you're getting paid for all the look-ups that are resulting from the abuse, that are resulting from your business practices, that would be a bad system.

GINA BARTLETT: Thank you. I'm going to propose let's walk through. I'm giving each person two minutes, and then we'll open it up for discussion and questions. Bear with me. ALAC, you're next.

ALAN GREENBERG: If I can read what I wrote. We just put a number of issues that we have to consider. Clearly, there are going to be costs associated with setting this up, operating it and so forth. There's also potential

cost savings. If we build an automated system, there's certainly a cost associated with it, but staffing the manual system also has a cost that has to be factored in. That's cost savings, at that point. It's not clear to me, by the way, when we're talking about this, how the costs get passed on. If costs are incurred by a registrar but paid by the requestor, the paid by the requestor's easy. It's not clear who funnels the various money from the registrars and registries, and who coordinates all that. What's the clearinghouse? That's not at all clear.

It's clear there will be a cost per request, with the consideration of public interest issues, as Mark was talking about. The pricing structure may be different for different people. It seems inevitable that some costs are going to be passed through to the registrants. This is a cost of doing business for the registrar and registries, and it's not clear why they should not bear a part of this cost, just like they've already incurred, and will continue to incur, huge costs associated with GDPR implementation in general. This is just another aspect of GDPR implementation, and it's not clear why it should be free at that point and only borne by the requestor. I'm sure once we start having models, we'll have more comments, but that's it for us right now.

GINA BARTLETT: Okay, thank you so much, Alan. Non-Commercial Stakeholder Group? Milton, did you want to lead on that?

MILTON MUELLER: I will. The policy principles under which our approach is based are not actually stated up there, because they were too complicated and you probably couldn't read them anyway. Our basic principle is just that cost should be based on actual cost causation. Whoever causes a cost should pay it, fundamentally. The other thing is that there should be a distinction between access and usage costs. There are flat fees associated with access, and there are incremental fees associated with actual usage. This is a well-known principle in pricing telecommunications, for example, that we should adhere to here.

Once we've got those as principle, then the challenge becomes let's identify the actual costs we're talking about, and then we can say who fundamentally causes them, and who they can be assigned to. With capital costs, this very much depends on whether we're talking about a centralized thing with an infrastructure or not. If we are, then possibly users are the real cost causers there. They're the ones who want an infrastructure, and they should provide most of the capital costs of setting it up. In terms of accreditation costs, again, that's something that benefits the user in a way I'll explain later.

There could be competition in this market so that you wouldn't have inflated costs, so that if accreditation was what we wanted it to be, which is merely authentication as to who you are, various firms could compete to provide this accreditation, hopefully avoiding the monopoly problem. We're thinking about a flat fee for accreditation that would be renewable over a time period, maybe two years or a year.

In terms of usage costs, those are clearly something where, in terms of cost causation, somebody who's not accredited would have to pay more than somebody who is, because the accreditors, number one, have already paid an access fee, and number two, they are easier to process. We do want there to be an option for people who are not accredited.

In terms of insurance costs, this is something that Thomas raised. We think it might be an issue, we have no idea where the money for that would come from. Something to think about. In terms of audit and enforcement costs, we're thinking that ICANN might have to shoulder those, but we're uncertain about where the proper place to put that is. It could be the DPAs. Maybe if they make money on their fines they would be able to cover those costs.

GINA BARTLETT: Okay, thank you Milton and Non-Commercial Stakeholder Group. Contracted parties? Yes.

[JAMES BLADEL:] Hi, thanks. I think there's some head-nodding with some of the things that have been presented already. Thanks for outlining the costs, noncommercial folks. Contracted parties, I think, wanted to lay out some high-level principles. I think the first being an agreement with the idea that this should not be a for-profit service, or any kind of a revenue-generating enterprise. We want to establish, first and foremost, that the costs should be neutral. I think that's a different way of saying the same thing.

Also, not borne by contracted parties or by the data subjects/registrants, but instead borne by the beneficiaries of the system, which would be the requestors. This should not be any kind of hidden fee or hidden tax which would be the result of, for example, assessing the operators of the system, or asking ICANN to foot the bill, because they're going to pass that through to contracted parties and to data subjects.

We also wanted to recognize that there are nonmonetary costs in setting up and maintaining this system. A lot of registrars and registries have a team that basically babysits our integration with the Trademark Clearinghouse to this day. That is a non-monetary cost, it doesn't appear on any product roadmap. Nobody wants to be hired to do that as a software engineer, okay? That is a reality, as Alan said, a cost of doing business. Our cost of doing business, our contribution to this, is the people that make this whole thing run. [We can trace it to a portion of their time.]

I think that that's what we're trying to establish. I think it's an important point, at least from a registrar perspective and a retail registrar perspective. It may differ for corporate and wholesalers. Domain names are becoming, or are, the least profitable, least marginal and most highly regulated part of our business, to the point where people can't get out of this fast enough. This could push people over the edge. This could convert more folks into resellers, drive more folks into areas where perhaps, if they wanted to create a shell company somewhere and offshore this so that they wouldn't have to bear these regulatory burdens …

I'm being a little wild now, but we've seen this happen where folks are moving to the Caimans or whatever to get out from some of

these burdens that we're putting on them, the reason being because we're talking pennies. If we pick up the phone once, or if we have to respond to a data request, we're already underwater on that customer and on that product, which is why you see the emphasis towards other more value-generating service models. It's very important that we not take the data subjects, who do not derive any benefits from this, or the contracted parties who are trying to serve other needs, like hosting, e-mail, site development, whatever, and then layer this on top of that cost structure. It will break the economics of this industry. Thanks.

GINA BARTLETT: Okay. The GAC?

ASHLEY HEINEMAN: Yes, we kept ours very principle level, here. As already noted by James, any finance model should not be profit or revenue-generating. We also indicate here that the system should not provide financial disincentives to requestors acting on behalf of public authorities. Something else we didn't capture here but we discussed quite a bit is that most governments have processes in place where you can request information from the government, and we have language associated with that, as well as cost structures that perhaps we could pull from as examples. We don't have a whole lot of detail to show you, but that was an interesting little corollary to this.

Also, what we discussed is that the whole intention of a unified access model is to provide efficiencies, and that's on both the

requestor's side, as well as intended for the contracted party side. It doesn't really fit here, but it's something I think worth raising that we're trying to minimize costs here, so when I hear folks start talking about the overhead at the registrar level, and the need to bring on lots of bodies and eyeballs, that makes me a bit concerned. Keep in mind that when we're developing this model, we're also trying to minimize costs. We should keep that in mind as we move forward. Not so much a comment to the system itself, but just something to keep in mind, to try and keep costs down as a part of this exercise.

GINA BARTLETT: Thanks to the GAC. Alright, SSAC?

GREG AARON: Hi. There are three places where costs might be located. One is in that central system, the meat in the burger. Somebody has to build and maintain that. One possibility is that ICANN pays for it. There are some precedents for it, for example the Centralized Zone File Access System, where we needed to have people who are consuming data get hooked up with people who have the data, and provide it, have an obligation to provide it, and make it more efficient for them to exchange that data. ICANN pays for that centralized system and everybody benefits. That's part of ICANN's job, to provide coordination.

There's been a long-standing concept, and SSAC wrote about this in SAC101, which is that providing RDS is one of the core services. That's always been assumed to be something that is

core to what the registries provide. That's mentioned in the contract. Registrars still have to provide Whois, because we still have use … Been issues, for example. That is something that they have to budget for, it's part of their costs. That's how it gets paid for, and that's, in a way, not our business. ICANN is not a price regulator.

We're, a lot of times, not qualified to get involved in the workings of the market, and there's a tension of, if we start thinking about designing these systems, are we qualified to do that? Do we let the market work where we're able to and have costs like this borne appropriately? We don't know what the answer to this is.

There's also another tension, which is purely from the security standpoint. The people who deal with security problems are mainly dealing with malicious registrations, where somebody has registered domain names and they're using them for abusive and criminal purposes. There are at least ten million of these registered every year.

These are problems basically caused by registrants, and they're somebody's registrants. The registries and registrars, these are their customers. There's a tension therefore of, should we have a lot of new costs associated with dealing with those problems? The people who have to deal with the problems in some models would have more costs to access this system. They're dealing with costs caused by somebody else's customers. We don't know how to deal with that, but we need some fairness and balance in whatever solution we come up with. Thanks.

GINA BARTLETT: It appears that the common threads are that any financing model should not be profit/revenue-generating, or cost-neutral, and to provide some incentives for cost reductions and cost savings. It appears where there's differing viewpoints is, who bears the cost? The beneficiaries, or is it shared more broadly among large users? There's concern around the per request basis, but others think that might be that the requestor might be the logical home for that. Non-commercial has broken up the cost in a more distinct fashion, with some question marks. Milton.

MILTON MUELLER: I just don't know what you mean by cost-neutral. Can somebody tell me that? There's going to be costs.

GINA BARTLETT: Cost-neutral I understood … James, you want to answer? You frame that term.

JAMES BLADEL: Yes, it's something I think was used or borrowed from the new gTLD application period for some of the things like the Trademark Clearinghouse, I think generally meaning cost recovery. For example, what Ashley was saying is there shouldn't be an incentive to providers to run up a score on this system. On the flip side, there shouldn't be a penalty for participating in the system, or disincentive for responding to requests. That means that whatever is occurring in this, if providers are incurring some kind of a cost, we should have an avenue for recovery. I think that both sides of that is that we don't want this to be a service center.

MILTON MUELLER: Okay, but to me the concept of cost-neutral is fundamentally at odds with our principles, which is that cost causers should pay. That means that people who don't cause costs shouldn't pay. That's not neutral, that's allocating costs based on who causes them.

JAMES BLADEL: Cost-neutral to the data subjects, cost-neutral to the providers, how about that? Does that clarification help?

MILTON MUELLER: I just think we should dispense with the term cost neutral. I think it has no basis in … Nothing is cost-neutral in the world of economics.

JAMES BLADEL: I think that's compatible with our first statement, which was that the beneficiaries of the system should bear the cost of the system.

GINA BARTLETT: Okay. Mark SV, Brian, and then come to Alan. We're really just open for discussion on all the proposals, and remember the charge of your work today is to frame up policy principles and implementation guidance for the staff to be able to write it up. We're open to discussing everything on the table. Mark SV, Brian, Allan W, and then Georgios.

MARK SVANCAREK: I think one of the disagreements that we have, and Greg touched upon this, is that we don't have the same definition of who is the beneficiary of the system. Greg was putting forward that we are all beneficiaries of the system, because the activity of bad registrants impacts all of us in some way or another. Some of us bear those costs differently than others, but we all bear some sort of cost, tangibly or less tangibly. When we say the beneficiaries of the system, it's not necessarily the people who are requesting the data for disclosure. Speaking of Microsoft, we're losing money on the whole process, all from one end to the other. We don't feel like we caused any of it, and a lot of the stuff that we're doing, it accrues to us just reputationally, if anything. I do want to be careful about defining the beneficiaries of the system as just simply the people requesting the access to the data. I think we're all beneficiaries of the system and that's why I use the term cost-sharing. Thank you.

GINA BARTLETT: Thank you. Brian?

BRIAN KING: Sure, thanks, Gina. We agree that the question about beneficiaries of the system is really open and certainly not just the requestors of the data. I think we need to really emphasize that a volume-based or a query-based or a domain-based billing model for this is really inappropriate and further penalizes the folks that are already being victimized by the bad actors in the DNS.

GINA BARTLETT: I'm sorry, Brian, did you say you support it or you don't?

BRIAN KING: Support what?

GINA BARTLETT: The volume thing.

BRIAN KING: We do not support the volume-based … Yes. That has a really weird impact on the companies that are the biggest victims that need to pay more to address their harms. Really weird. I think that's probably our biggest two points right now. [I'll do] the rest of the conversation.

GINA BARTLETT: Allan W?

ALLAN WOODS: Hi. I'm just going to drop one slight bombshell that I think needs to be overall on this, and that is that we need to do a cost-benefit analysis as well, as to all the cost that's going into this system that we're creating. If it turns out that it's just not worth it, then we need to come up with a different system. That might very well be the decentralized system. It's not a centralized system and that might very well have to be where we go on this, because we're not going

to be spending 100 million for a small benefit. We have to be very careful on that one.

The second thing is, and I heard this from Mark, where you were saying that this has to be passed onto the registrant, but let's just break that down. The registrant is the data subject, and what you're saying there is that the data subjects might ultimately bear the cost of us disclosing their data.

MARK SVANCAREK: Actually, I don't that was me who said that.

ALLAN WOODS: That is kind of what you said. You said that the registrants will ultimately have to bear the cost. I'm sure I heard that. Anyway, I would also add a little area to that, and contemplate how would that affect the 6.1(f) balancing test? Because it wouldn't be in your favor, because that has a material impact to the data subject as well. Again, these are all very baseline concepts that we need to be careful of. Therefore, that's why we would say that we should not pass that on to the registrant at all, we just need to avoid that.

MARK SVANCAREK: If I can come back, I don't recall saying that, and if I did, I apologize for being ambiguous about something.

GINA BARTLETT: I've got Georgios. I have a big queue. Go ahead, Georgios.

GEORGIOS TSELENTIS: Yes, thank you. Just picking what was said by Greg, and also by Mark, I understand when we want to go to identify the cost causer, the principle that Milton said. I think if you take the analogy where you have bank systems where there is fraud, and you have a central system, it's a similar situation to me. You have something that has done harm, and then who bears the cost in this case? Who is the cost causer in this case? Are we talking now that something happened and the one who has to bear the cost is the one who is asking for the disclosure? Are we going a little bit further down the road, and we say that there is an issue, because there was harm to the whole structure of the financial system, or here the DNS system, that somebody has to bear the cost in order to alleviate the harm which was done to all the parties here?

That's why I believe we have the fundamental difference in the positions of the groups. Some people say that because somebody's asking something, then the cost should go to them. I heard what Greg said there. The issue is that they are asking because there was a harm that was done to the whole ecosystem. What is happening here is that we are benefiting from [lifting this] harm to the system.

GINA BARTLETT: Thanks, Georgios. I have James, Milton, Greg, and then I'll continue on.

UNIDENTIFIED MALE: And then Alan, and Volker …

GINA BARTLETT: I have a huge queue, I'm just doing … Alan G, you're on here. Here you go. I've got James, Milton, Greg, Volker, Alan G, Stephanie, Mark SV, and Brian.

JAMES BLADEL: Okay, I'll be brief, then. I just want to clarify, perhaps it would be helpful if we identify direct beneficiaries of the system, which are those making the requests, versus indirect beneficiaries, which is all the people who get to live in peace and harmony because there's no longer spam or fraud on the Internet. If we want to try to lump them all together and say that's why everybody should pay, I think that's where you're going to get pushback. The direct beneficiaries of the system should pay for the system.

GINA BARTLETT: Thanks, James. Milton? And if everyone can try to be concise, I think everyone would appreciate it, since we have such a long queue.

MILTON MUELLER: Right. This is really an area of my personal expertise. What you're saying, in effect, with this argument that we're all victims, it's a public goods argument. If you want to take that and pursue it consistently, the financer of the system should be tax revenue from the government. If the government wants to pay for this as a public good, that's fine with me, go ahead and do it. I don't think it's going to happen.

James is correct, there is a very clear distinction, here. A very clear distinction in terms of quantity and quality between a direct beneficiary. Frankly, it doesn't hurt me very much if some domain that has a trademark infringing … There's no direct harm to me. Maybe in some general sense, there's more fraud on the Internet, but most of the costs are private costs faced by the trademark holder, and the trademark holder is, as a general principle of law, responsible for enforcing their own marks. They are the cost causers.

The other thing is, when you're saying that the cost should not be assigned to cost causers, you're in effect saying that the rest of us, who don't have a direct stake in this, should be assuming these costs. It's not like the costs go away, okay? It's true, in some [inaudible] share the cost? Well, not most of it, no. Maybe my insurance rates go up in the neighborhood, but in general there are direct beneficiaries, and there are indirect beneficiaries. I think it's a matter of great importance, from a justice standpoint, to make sure that the costs are assigned to the cost causers, otherwise we have this cost-benefit calculation that gets really skewed, so that people who are direct beneficiaries of this system are getting all kinds of benefits, and the rest of us are paying for it in ways that are not really … It's a net loss, for us.

GINA BARTLETT: Thanks, Milton. Greg?

GREG AARON: I was doing a calculation, and doing a lot of Whois queries last week. A lot of the data that's being blocked right now is not covered under GDPR. The temp spec allows registrars and registries to block any records they wish. Some have chosen to display based upon whether they're registrants or their operations are in the EU. A lot of them are blocking data not for a legal purpose, but because they can. That means we have lost access to that entire set of data, which is probably bigger than the set of data that's actually protected under GDPR or similar law. The demand for that data is big, but there's not a legal justification, necessarily, for redacting it. We've lost access to data that's not protected. That's an issue, but we're not dealing with the geographic issues here right now.

There's also what I saw as a fair amount of noncompliance with the temp spec, potentially. I don't mean not responding to requests necessarily, although there may be some of that, but I saw it more as I can't get the contact means that are guaranteed under the temp spec. I can't see the address of a web form in the output, I can't see an anonymized e-mail address, either. You've got a system that's broken, pretty much, at this point. It's not working in the way it was envisioned under the temp spec. The system is going to have a benefit of making things uniform and predictable again, and may help solve some of those problems, as well. Thanks.

GINA BARTLETT: Thank you, Greg. I'm going to keep going. It sounds like this concept of thinking about the beneficiaries in the direct and indirect might be a way to help problem-solve and guide the policy

direction. Anyone who can speak to that, it would be helpful to hear your thoughts. Volker, Alan G, Stephanie, Mark SV, and Brian.

VOLKER GREIMANN: I'm sorry. Just two points. First point, Greg earlier talked about these abusers being our customers. Let me tell you about those customers. Usually, the first victims of these abusers are not people that fall into that trap, but the registrars whose customers they are, because most likely they're not paying with their own credit cards. We have chargeback fees, we have all kinds of fees. We have costs that have come into our books that we bear as part of our cost of doing business. These valued customers are already a cost factor, and adding an additional cost in the form of a disclosure process to that cost that we already bear is probably unwarranted.

The second part I wanted to raise is that I hear about all these costs that the victims of these users are now additionally having to bear. I see it differently. This is actually a saving for many of you guys, because what many IP owners and victims of fraud or other issues of abuse on the Internet currently do is go to their lawyers, the lawyers write a letter, send that to us requesting disclosure for certain information, or other bits of information that we might be able to provide. Not having to go to these lawyers and writing these letters, they're having to write these letters, not having to [have] your own legal department on that for hours and prepare a legal complaint, but rather having a simplified access model that will just provide you that data is probably a very significant saving on the part of the victim of such abuse. Therefore, I think the small

fee that allows us to recover our costs in providing that service to you is probably warranted as well.

GINA BARTLETT: Thank you. Alan G?

ALAN GREENBERG: Some of the statements being made around the table, I find a little bit outrageous. Sorry. Allan's comment about the registrant who should not have to pay if his data's being released. He's not going to pay a per use charge, we're talking about an infrastructure cost that's part of the overall system. We already bear it in fraud, on credit card. We all pay higher fees, pay higher interest. The merchants pay a higher fee because of fraud. It's covered uniformly, it's not covered by the individual user, as Milton said. Your insurance rates go up if there's a problem in your area. We all pay it, whether we like it or not. I don't see how we can end up not having some of the costs borne as part of the cost of doing business. Not all of it, but I just don't see how we're going to end up with a system that is fair and equitable without the cost being distributed. Thank you.

GINA BARTLETT: Thanks, Alan.

ALAN GREENBERG: I appreciate James' comment that this is not a high margin business, but that's why it has to be passed on, it can't come out of your margin.

GINA BARTLETT: Stephanie, thanks for waiting.

STEPHANIE PERRIN: Thanks very much. Having said that I think in terms of data protection we need tight parameters, I think in terms of cost redistribution we need to think much more systemically. It does seem to me we're going through a period, particularly with cybersecurity costs, that has not been allocated across the system. Everybody jumps onto the Internet. Various parties have picked up the job of policing these cybersecurity aspects. They may or may not get paid, but following the money – I'm not an economist, just like I'm not a lawyer – is really tough, here. Who's actually paying? How are we paying? Where are those costs covered? I don't know, but I don't think that for DNS information we should think just in terms of the ICANN box, but all of those costs have to be found within this system.

I think if we did a regulatory impact assessment, and so far I've got zero support from my colleagues on this, we would at least have a better handle on what the impact is of attempting to recalibrate costs in the light of the GDPR. If there's fraud on a website, not all of that is directly attributable to the DNS, you know? That's theft in a neighborhood, right? Those costs may come from somewhere else. Maybe the blessed credit card rates

go up yet again if a website gets hacked, instead of bringing it back here to the cost of running the DNS. In any case, we certainly can't drive up the cost of a domain name just over this. If it goes to the registrars and contracted parties, then it goes directly back to the individual. I think that's unjust.

When the financial crimes transaction reporting legislation came through in the western democracies, that didn't come out of the end-user, that came basically out of the government systems, right? They built the centers, they built the networks. They may not be working well, but at least it was a centralized function. I think we need that here, and we need to come up with some facts so that we can make an argument for that.

GINA BARTLETT: Thanks, Stephanie. Mark SV, I had you next. Are you passing, or?

MARK SVANCAREK: Actually, I don't think I was in the queue.

GINA BARTLETT: Oh, I'm sorry, I had you in. Brian?

BRIAN KING: Thanks, Gina. A couple of reactions. I agree with the comment that this is core to the system. This is core to the way the DNS works, and therefore the cost needs to be systemized, needs to be baked in. The best way to do that is to spread it out across the different parties involved, and in particular including registrants

and the folks that might become accredited to make that process a little easier. The IPC is not opposed to an accreditation fee to foot the bill for some of this, especially if that accreditation does help make the processing decisions easier, and enable access in a more streamlined, predictable way.

I would caution everyone here that the optics involved in penalizing the victims of cybercrime are very bad. When someone is being abused, or their IP is being infringed, and they go to find out who that person is, ICANN does not want to be in a position to say, “Oh, sure, we can help you find that out. Pay up.” That’s not good optics, or the way the world should work. Then, I would say that on a really fundamental basis, trademark owners are not the cost causers.

I don't know what we’re gaining by trying to figure out who the cost causer is, it could be the European government that passed GDPR, but it’s certainly not trademark owners. In that case, if they want to foot the bill, I think that still doesn’t help us because the power to tax is the power to destroy, so we can’t have them paying for this either. In any event, trademark owners are not the cost causers. In fact, the bad guy registrants are the cost causers, and I don’t know a way to make the bad guy registrants the only registrants that chip in for this, so it seems only fair that this is spread for the benefit of the entire ecosystem, across all the players. Thank you.

GINA BARTLETT: I'm going to come to you, Milton. Can someone help me? Where are you on this? What will work? Where is the policy that you

could coalesce around? That is your charge. What integrates all of these different considerations and concerns around the beneficiaries and the cost-sharing? Milton, you want to take a stab at that?

MILTON MUELLER: We are fundamentally at odds, there's no doubt about it. We're being given voodoo economics.

GINA BARTLETT: Let's not ascribe motivation or label people's points of view.

MILTON MUELLER: I'm not describing motivation, I'm describing a lack of –

GINA BARTLETT: Well, voodoo … Just try to be respectful, please.

MILTON MUELLER: This just flies in the face of everything we know about economic science. To say that the trademark owner who issues a disclosure request to a registrar is not causing the cost of responding to that request is fantasy. We know what cost causation means, here. It doesn't mean that the trademark owner is responsible for the cost caused by the cybercriminal, but we're not about eliminating cybercrime, we're talking about disclosing data about the registrant. Who is causing the cost of creating a system in which we forward information about the Whois record to that particular

person? Who benefits from that, directly? It's clear that the trademark owner is benefiting, and that they are creating the process, they are instigating the process that causes the cost. I just don't know how you can argue with that.

It's not like we want to penalize the victims. What we're saying is that costs of cybercrime are out there, right? The question is, you want to institute a particular procedure that helps in fighting it. By the way, every time you ask for a disclosure, it doesn't necessarily mean the person is guilty, it just means you're getting disclosure, and you can follow up with him, for example through a publically-funded law enforcement process, possibly. If the cost of making that particular procedure work is not caused by the person making the request, or that it's not fair to assign that cost to the person making the request, then how is it fair to assign it to me, or GoDaddy, or the registry? How is that fair?

The registrars are going to pay for part of this system. They're going to have to integrate their systems with it, they're going to have to assign staff to respond to requests, and nobody wants them to be making a profit on these requests, but if we want to have a rational, efficient and fair system, we have to assign costs to people who create procedures that cause costs. I don't see any way around that. Just to answer your question, this is a fundamental principle and we're completely divided on it. I don't know how we're going to resolve that.

GINA BARTLETT: James, Volker, Mark SV.

JAMES BLADEL: Yes, I'll be brief and just say that I think Milton's on to some important points. We're not going to get anywhere if we start throwing all the costs we can possibly think of into this. The costs of fraud on the Internet, the cost of the CO2 to run the servers. We can keep blowing this up, guys, to the heat death of the universe and entropy. We're talking about the cost of providing and making available an investigatory tool to users of the system. Law enforcement, intellectual property, cybersecurity, those are the big three. We're providing this facility, and I don't think it is outrageous or unfair or somehow unjust to say that that the users of this facility should pay for that facility and the heavy users should make a larger contribution.

I think that is just so commonsense, I'm struggling with why we're having such a hard time wrapping our minds around this. I think the concern is that we're operating in an environment where all this stuff used to be free. We know from the tragedy of the commons what happens to a free resource. What we're trying to say now is, this external thing, privacy law, has said this cannot be free anymore, you have to protect this.

Data is the new oil, we've all heard that. We have to be mindful about how we're providing it. I think that if we tip this up so that registrars … I'm not talking about my registrar, I'm talking about just generally, if registrars and registries have to make a fundamental decision about whether offering or participating in this ecosystem, or continuing to, is going to flip them over on their income statement, that's not an outcome that we want, either. That's going to lead to consolidation, that's going to lead to fewer

operators and less diversity, and underserved markets and all that stuff.

Let's be very clear, we're not trying to boil the ocean and solve every cost we can think of. We're talking about the cost of deploying and operating an investigatory tool and a service. If we keep things focused on that, I think it's very clear who the beneficiaries are. Yes, thanks.

GINA BARTLETT: Thanks, James, for that narrowing and clarification. Volker? Then I've got Mark SV, Alan G, Stephanie, and Thomas.

VOLKER GREIMANN: Yes, everything that Milton said, and James said, plus the potential savings that the beneficiaries of the system are actually entitled to gain. I think we should not look at the Whois as it was, we should look at the status quo as it is now. There is no more free service to look up that data, you have to find a means to either write to the registrar to request disclosers, send a legal letter or whatever. I still feel that this process, if we establish it, gives the beneficiaries a large amount of security of process, ease of filing these requests, a lot less disparity between the responses that they're expected to get, and the potential to cut costs significantly for receiving those answers.

If that is something that we cannot coalesce around, the only other potential I can see is that we stay with our current decentralized system and create a system of guidelines and rules that every party will have to follow, the requestor as well as the contracted

parties, to help us guide, or guide us to making or responding to requests, and create a certain code of conduct around that. That wouldn't be a centralized system as we are envisioning right now. That would be the other option. If we cannot align on costs, it would be something based on what we have now, just with more rules around it.

GINA BARTLETT: Mark SV? And if you could help us bridge, and think through your interests and how they blend with others, thanks.

MARK SVANCAREK: Sure. One thing I'd like to caution, I think we're starting to slide into attributing motives to people. I've heard a lot of, "This used to be free, you want it to be free again." That is not true at all, we recognize we are building a brand-new system and we are establishing the parameters for a brand-new system. What happened in the past is not really material to this discussion. I point out that the CSG principles did not say that users of the system would not pay, it simply said that there would be some sort of cost-sharing, and that the proportionality of it should be figured out based on a bunch of parameters, as opposed to, "This party pays the whole thing, this party pays the whole thing."

As Milton points out, the use of the system by trademark holders is different from the use of the system by somebody who's investigating bank fraud. That's a great example, I think. If Microsoft is investigating bank fraud, I don't see how Microsoft is a direct beneficiary of the system except in the general way that

James talked about, the whole ponies and fairies and unicorns and everything is safer … I know, I'm sorry, I don't remember exactly what you just said. The general system of everybody's safer, blah, blah, blah.

We recognize we're users of the system. We have to pay something. We're worried that all the costs will be passed through to us blindly, because then there's never any incentive to make it better. We think that some people should pay more than others. We acknowledge that. We do think that there should be some shared pain, though. When we talk about pure cost-neutrality, maybe that was never an issue.

Maybe, as James says, there's so many intangible costs that registrars are going to be paying … You know what I mean? If the principle is registrars must recover all of their costs, all of the time, hopefully that isn't what you were saying. Good, then let's drop that, because that, maybe, is no more true than the assertion that users of the system don't want to pay anything, or want to pay us at all, to the registrants. I think perhaps both of those are incorrect assertions that we should step aside from.

UNIDENTIFIED MALE: Just very briefly, I don't think anyone has made that claim, first.

MARK SVANCAREK: Okay, good.

UNIDENTIFIED MALE: And then secondly, one of our fourth ones up there is to recognize that contracted parties are going to make intangible contributions of resources, mostly developer time and engineering time to this, that are just not going to be recoverable. Recognizing that we're not running the meter, let's say, on our developers, but that should be, and that is, our contribution.

MARK SVANCAREK: Okay, so I think we've now eliminated one of the roadblocks that we had towards understanding. I think there was an acknowledgment that people who use the system are going to pay something, and that contracted parties are going to be paying part of the cost. They're going to be paying something as well, so I think we can step that aside. We were starting to go down that path of, "You want this, and you said that." I don't think it was true, and it was starting to become distracting. That's all I wanted to say for right now.

GINA BARTLETT: Thank you, Mark, and thanks for the reminder to not ascribe motive. I'm going to Alan G, Stephanie, and Thomas. What I think I hear as a guiding force is what we're talking about is the cost of providing and making available this investigative tool and service. There are benefits associated with that, numerous, but a few that have been called out are certainty to process, cost savings associated with that certainty, and not needing, maybe, individual inquiries with attorneys contributing. And, that people support a cost-sharing device, or cost-sharing system, recognizing there's direct and indirect beneficiaries. Some may pay more than others,

and the costs need to be shared across the system. I think the question is, what are the guiding principles around that? Is it by volume, by player, by responsibility? Where does that fall? Let's keep building on that. Alan G, go ahead.

ALAN GREENBERG: Thank you very much. There's two potential classes of the system we haven't discussed here at all, and I don't think the same rules will apply. It's not clear you're going to get law enforcement to pay, at least not in most worlds that I'm familiar with. Second of all, one of the classes of users of any systems we build, which we haven't talked about at all, is ICANN. Not a third party, but ICANN makes a whole bunch of requests, typically from Compliance. I don't think we're going to build a system and then say we're going to build a parallel system for ICANN to use privately, therefore ICANN's going to be one of the large users. We need to factor that in. As purely an aside, one day I'd like to have a discussion in ICANN about how to eliminate domain abuse, instead of how to pay for it.

GINA BARTLETT: Thank you, Alan. Stephanie?

STEPHANIE PERRIN: Usually, I agree with much of what Alan says, but unfortunately today I don't seem to be. We haven't decided whether ICANN is controller or third party yet. ICANN may very well be a third party with respect to the system if it refuses the controller role, so that GDD will have to start paying for access. We haven't determined that enforcement mechanism.

I wanted to follow up on something that Volker had said. James said much of what I wanted to say, so I won't repeat what he said. Volker pointed out that we may not have a system. We may have a distributed system. Were we looking at this in a logical order instead of backwards, instead of having the engineers come up with a hypothetical SSAD, and then have us figure out whether we can afford it, the first step is to figure out procedures of how we are giving access, and then we try to do a cost analysis of how we pay for that, and where those costs go. Then, we move to a bigger, more complex model, i.e. the SSAD, and see whether we can afford it. Now, I don't think we've got the data to do a proper cost-benefit analysis right now, but if we were going in logical order and developing our templates and our procedures, then we could stop when we ran out of money, instead of going the other way around. Please, let's think in that way.

GINA BARTLETT: Thanks, Stephanie. I've got Thomas, Volker, Mark SV. No, Volker's done. Then, maybe we'll check-in and see what our next steps are, because we're about to lunch.

THOMAS RICKERT: Thanks very much. I think once the decision is made in this group, or in this community, that an SSAD is going to be built, I think there is acknowledgment that we need it. Again, this decision has not yet been made, but if everybody around this table comes to consensus that we need it, then I think that should go with the understanding that each of the stakeholder groups who presented here will have to contribute to the cost of setting this up, and the

burden to set this up. I think maybe that can be one of the guiding principles for attributing and distributing cost.

At the same time, I think we should really keep the discussions of setting up this structure apart from the usage of the system. When it comes to usage of the system, I think there are examples outside ICANN's world where we can probably learn from. Law enforcement, in many cases, has to compensate ISPs for providing data and responding to disclosure requests. That is factored in in other areas. Or working on trademarks, if you are asking public registers to come up with data. You pay for those, but you're able to pass on that cost in an infringement case to the infringer.

I'm not saying that we have to copy exactly what's being found in other worlds, but you find examples of where disclosure requests are being paid for at the moment, and then you can make a distinction between egoistic motive … That's not what I'm saying, but if you look at legal literature, somebody who wants to protect their trademark, i.e. having an exclusive right in a certain string, and protecting that, is to be treated differently in certain aspects than, let's say, a security researcher who is following altruistic motives exclusively. I think we should probably keep those general silos, let's say, in mind when talking about the allocation of costs, and also look at the type of information returned.

If you're looking for personal identifiable information for registrants for certain cases, that's different than, let's say, a security researcher investigating a network attack. That person might not be even interested in personal data but just statistical data on how many domain names, or how many objects, are associated with

the requested data. I think we need to be innovative on what we're actually discussing, what the benefit is, where the costs can be passed on, and so on.

GINA BARTLETT: Thank you. Go ahead, Mark SV.

MARK SVANCAREK: Thomas, thanks for explaining all that better than I could. I also just wanted to recognize there's a bunch of people who've made reference to cost-benefit analyses. Stephanie was the latest to do it, but I think Allan Woods did, a couple of other people did, and so I just wanted to support that concept. I think it is going to be critical, and I find it very daunting because it's premature at this point. It's this looming responsibility that we're going to face that right now just seems big and insurmountable, but clearly needs to be done.

GINA BARTLETT: Thanks, Mark. I'm going to look at Marika and Janis as far as, where do we go from here on this item? We've heard some clarity on the framing of the setup and the use for the cost, and then cost-sharing ideas, with a need for the cost-benefit analysis, but what would you recommend?

MARIKA KONINGS: Thanks, Gina. I think from a staff perspective, we can really try to incorporate some language in the zero draft, or the next iteration,

recognizing or making clear that it's not necessarily yet agreed, but maybe that reflects some of the points made here. I think there's, as well, some suggestions more on the implementation side that we can also uplift and mark them for further discussion. I think some have noted that we may only be able to come back to this once we have a clear idea and lead on what SSAD looks like, so you can have that in the cost-benefit analysis, and that may make it easier, as well, to wrap up this conversation and come to an agreement on the recommendations, as well as any implementation guidance that the group wants to provide.

GINA BARTLETT: Does that sound good to folks? Okay. I think it's time for lunch, right?

JANIS KARKLINS: Yes, thank you very much for this conversation. I think that gave all of us a certain sense of direction, and at least a way of thinking. For me personally, I think a way forward would be also to think in terms of splitting two processes and try to think about funding of those separately, meaning creating of the system and then running of the system as Thomas suggested. The cost-sharing structure certainly might be different in both. We will try to do our best in writing up and proposing a version in 1.0 draft.

I also can confirm that it would not be unusual that law enforcement is paying. I think I said something on one of the calls. I heard this discussion on Swiss radio, that law enforcement bitterly complained that Swisscom is charging too much to Swiss

law enforcement for access to court warranted telephone conversations. That wouldn't be anything extraordinary, if law enforcement also would participate in cost-sharing schemes. The question is how much? I think this is the balancing moment that we need to think about, and make sure that this is also perceived as a fair distribution of running costs of the system.

Now, lunch break. Please, during the lunch break, refresh your memories on the two legal memos, and the third one has been distributed or will be sent out immediately now, because that came in about an hour ago. We will not specifically address the third. We will be focusing on the first two that were sent to the team last night. After that, we will again enter into a kind of brainstorming discussion about the systemic issue, where the balancing act or decision of disclosure should be made, and different options. Again, not decisive, but simply to get the feeling of how we think about it, where it should be made. Please, try to already tune your minds for that conversation. With this, bon appétit, lunch is served. We're back at 13:00, as suggested in the program.

[END OF TRANSCRIPTION]