ICANN Transcription

EPDP on the Temporary Specification for gTLD Registration Data

Thursday 13 June 2019 at 1400 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
https://icann.zoom.us/recording/play/e7zTGEY8-E5IKoDtCUIsAvynS5TQYG8pDN1RXW9lOEhD17Et4Q4MnN617iF3NdNd

Zoom Recording: https://icann.zoom.us/recording/play/wwY1GBJv-qnYNrueMGEDWgA8cNlewLdAHIMvAZgv4JZvuApGOREWY6FGg-mRzhcn?startTime=1560434454000

Attendance is on the wiki page: https://community.icann.org/x/7ISGBg

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page:
https://gnso.icann.org/en/group-activities/calendar

TERRI AGNEW: Good morning, good afternoon, good evening, and welcome to the sixth GNSO EPDP phase two team meeting taking place on the 13th of June 2019 at 14:00 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken via the Zoom room. If you're on the phone, could you please identify yourselves now?

Hearing no one, we have no listed apologies for today's meeting, but joining a little late will be Chris Disspain of the ICANN board. Alternates not replacing a member are required to rename their line by adding three Zs at the beginning of their name, and afterwards, add your affiliation, dash, alternate. This will automatically push you to the end of the queue. To rename in Zoom, hover over your name and click "rename." Alternates are not allowed to engage in the chat apart from private chat, or use any other Zoom room functionality such as raising hand, agreeing or disagreeing.

As a reminder, the alternate assignment form must be formalized by the way of the Google assignment form. The link is available in the meeting invite e-mail. Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now.

Seeing or hearing no one, all documentation and information can be found on the EPDP Wiki space. Please remember to please state your name before speaking. Recordings will be circulated on the mailing list and posted at the public Wiki space shortly after the end of the call. Thank you, and with this, I'll turn it back over to our chair, Janis Karklins. Please begin.

JANIS KARKLINS: Yeah, thank you, Terri, and good morning, good afternoon, good evening to all. This is our sixth meeting, and proposed agenda of the

meeting is on the screen. Any comments? May I take that we wish to follow our proposed agenda for today's meeting?

I see no reactions, so it is so decided. So let us turn to item three, subpoint working definitions. As we discussed last time, the working definitions have been amended as we discussed and are posted now on Wiki. So I think this is now our reference document with understanding that the one proposed definition was not being endorsed, and that was on access. Any comments?

Subpoint two, legal advisory group now we renamed it last time to legal committee, which is representative, and I asked all groups to forward a name of representative. And if I may ask now secretariat to put on the screen the nominations that have been submitted so far.

So now you see representatives of groups that we have been nominated by their respective groups to work in the legal committee, and so is there anyone who wants to say anything at this moment? Marika, your hand is up. Please.

MARIKA KONINGS: Yeah, Janis, I just note that I think there were a couple of names that we haven't added here. I think Margie also put her name forward. So I think we need to reconcile the list, because I think we had some submissions that were sent directly to some staff members. Some went to the list. So I think if others can confirm in the chat if your names are not listed here, I also know that of course, based on the original proposal of the small advisory team and committee, and there were a couple of names that had been approached, we just need to make sure as well that we

confirm that those representatives are also still willing to serve on behalf of their groups. So maybe if we can take the opportunity for – I see some hands raised already, to kind of confirm and have anyone else missing here, we can add them. And I see some [already know] in the chat. So hopefully, we can complete that.

JANIS KARKLINS: Okay. Thank you. We have now two other names. And my apologies, Margie, it was simply my omission. You sent to me and I omit to forward it to staff. My apologies. So now we have Laureen. I think Georgios wanted to present or nominate Laureen. She's on the list. Thank you. Now I have Amr. Amr, please go ahead.

AMR ELSADR: Thanks, Janis. I'm not sure where we landed on in terms of representation of the group. And I apologize. I've been away for a while, and I'm just starting to catch up on past couple of days. But I do believe that NCSG members have expressed concern with the number of representatives from each group. To me, this goes more than just the issue of balance in representation between for example the Noncommercial Stakeholder Group and the Commercial Stakeholder Group. But it's also a matter of practicalities. In the past, during phase one, it was challenging for NCSG having one rep on that group, which was a committee back then, I think, and we kept switching in and out, for example Tatiana was the representative for the NCSG on that committee, and at times when she couldn't make it, I would jump in, and then I would jump back out. She would jump back in. We would try

to coordinate and update each other effectively, but from a practical perspective – and again, this is apart from the arguments on representation, which I won't repeat, but it has already been stated.

But from a practical perspective, I think it would be very helpful for the NCSG to have two or three members on that group, not just for issues of balance but also just to make sure that our group remains on top of things and we can coordinate more effectively as a team. I hope the EPDP team will take that into consideration. Thank you.

JANIS KARKLINS: Yeah. Thank you, Amr. We had conversation, and we started with the idea of alleviating very heavy duties of team members by – I propose to select small legal advisory group which would examine questions and would put forward the proposals to the whole team. It was not supported, and we came to another proposal which was to make representative legal committee where each group would have one representative.

One means that if nominated representative cannot make a meeting, then somebody from the same group would step in, replace that. But in any case, whatever legal committee will decide or will recommend, will come for adoption and endorsement to the team as a whole. So therefore, you should not be worried that the voice of your group will not be heard, and in any case, the whole team will approve whatever recommendations will come out from the representative legal committee. So therefore, if you want to nominate Tatiana and you as a member who would replace in case Tatiana cannot participate, fine.

This is a working arrangement. And again, please, the whole idea behind legal committee is to alleviate workload of the team as a whole.

So first, Georgios, then Amr.

GEORGIOS TSELENTIS: Thank you. I just wanted to say that my understanding for the whole arrangement was, okay, we secure representativeness of the different groups, but at the same time, we want to be efficient as you mention, Janis, and I think we should strive for how to get the maximum of the legal counsel. And for me, the added value that we have is not necessarily on the outcome or what are the conclusions, but it's primarily on the background work that legal counsel is conducting for topics that we find that are important, and it does all the legal analysis of those issues, so when we get those memos, we have much more information to take a decision on those issues in an informed way.

So that's for me the added value, is not to prejudge or to guide or to limit the opinions of the groups. So I think in one way, what is suggested in the representativeness is going to respect it, and therefore, I think for us it's fully workable that somebody can step in in the group to be represented, but for me, the added value – and please confirm this – is on the analysis that is provided by the legal counsel ,and if it is well digested, then the group can make much more informed decisions. Thanks.

JANIS KARKLINS: Thank you, Georgios. Amr, please.

AMR ELSADR: Thanks, Janis. Following up on your response to my earlier comment – and before I do, I just wanted to thank Mark SV for expressing a nonobjection to multiple NCSG members being on the committee. But if a decision has been reached that only having one member from every group, whether it's stakeholder groups or constituencies being represented on the committee, would an agreeable compromise be that a mailing list be set up for this group and that even those who are not the primary representatives of their groups have the ability to subscribe to it?

Again, I'm looking for practical solutions to this just to make sure we don't drop the ball, and having real-time access to e-mails being shared as well as documents and discussions will make it more helpful for our group, for the NCSG at least, to be able to have one person jump in to replace someone else, just to make sure that all our team members are continuously engaged with the work of that group. I hope that would be an acceptable compromise. Thank you.

JANIS KARKLINS: Certainly, Amr. Thank you. I think we have adopted from the very beginning the open door policy in general, so the meeting of representative legal committee will take place with open doors, so everyone will be able to join the call.

Of course, not everyone will be able to speak, but at least listen. I have no problem constituting a mailing list which contains as many names as needed, so this is just a mailing list, but the whole point of this group is

to save time to all the members of the team, and as Georgios said, to prepare issues for consideration of the team as a whole that the team can take the best decisions in the shortest possible time when it comes to legal questions.

So with that understanding, we would then expect nomination from NCSG, and we would proceed as we discussed. Good. So next agenda item on the list is the worksheet on SSID. And if I may ask Marika to kicksstart or to update us where we stand with that worksheet.

MARIKA KONINGS: Yeah. Thank you very much, Janis. You may have seen an e-mail go out at the end of the day yesterday in which we noted that we've posted the updated version of the SSID worksheet on the Wiki page where all the other worksheets are posted as well. You'll find there are actually three different versions there, one of which is the clean version, one is the redline version, and then the third one, which is the archived version which contains all the comments and proposed edits that were made on the original Google doc, as we outlined in the e-mail and also discussed during last week's call, for the updates we made, we really focused on those comments that specifically went to changes to topics, how they've been referred to the scope of the issues as well as order of topics.

We noted that there were quite a few comments that either suggested specific suggestions or changes to charter questions .we don't think at this stage it's appropriate for staff or the group to make those changes, but of course, over the course of deliberations, the group can explain if

there are specific nuances that the council should take into account as the group provides its response to those charter questions.

Similarly, there was a lot of substantive discussion through a comment which of course is very helpful and good, but not necessarily, I think, intended to change the current format of the worksheet. But as such, we kept all the comments visible for you in the archived version. So I just would like to encourage you to please have a look at the updated one, either the redline or the clean one, to see if there's something we've missed. From a staff perspective, I think most of the specific suggestions that were made were all helpful and constructive, and hopefully not of a controversial nature.

One thing I would like to do and remind you all of, you should have received an e-mail from the GNSO secretariat asking you for your Google account e-mail address, and we've had some issues with unauthorized removal of comments from some of the documents we've posted, because so far, we've used a link that people could click and basically on the honor system, have only members provide comments or edits. But we've had some others go in there.

So now going forward, we'll set up a new Google document that requires EPDP team input, will set them up with your specific Google accounts so that only those authorized are able to add it and provide comments. So please make sure to get your information to the GNSO secretariat for those documents that are still open, which I think is mainly the worksheets. We hope to make that switch by the end of the week, so please do so, otherwise you may not have the appropriate access. That's all I have.

JANIS KARKLINS: Okay. Thank you very much. Any questions, comments? I see none, then we take note then on the update. As we discussed, the worksheet will be a living document, and it will be amended as we progress in our conversation, either with the background information or whatever decisions we will manage to take.

So with this, we can move to next item, and that is SSID topic. Before giving floor to Marika to introduce the document which was distributed two days ago to the team, I would like simply to recall that during the last meeting, we were examining initial proposal on the groups, and it was requested or strongly suggested that we should start by defining purposes of disclosure and the purpose then would define also or would lead us to the definitions of the requestors or different groups of requestors.

So with this document, we tried to follow the suggestion and see whether this approach will get traction, and we will be able to progress in our conversation and in defining and developing those building blocks of the SSID that we're attempting to develop.

With these words, I would like to invite Marika to kickstart the discussion.

MARIKA KONINGS: Thank you very much, Janis. I'm just going to pull up the document for those wanting to see and being able to scroll through it. You may prefer to open your own version which was circulated together with the

agenda. and as Janis noted, this document is the result from last week's conversation where we originally had taken the approach to focus on the user groups and work our way down from there. So this document has kind of turned it on its head, and instead focused on third-party purposes or legitimate interests for requesting disclosure of nonpublic registration data.

We tried to provide a little bit of an intro as well in the document [inaudible] where the information in the document comes from. We specifically looked at this document, the link was here, and I think we included as well a required leading list, which was the result of a request from ICANN Org at the end of June 2017 requested the community to identify [user types] and purposes of data elements required by ICANN policy and contracts.

[So we ran through that list, we did observe a number of instances.] It was more focused on the original, pre-GDPR use of data, so we made in certain cases some kind of an assessment and following as well conversations we had [inaudible] what would be indeed third-party purposes for requesting access to data.

We also highlighted here that the [inaudible] phase one recommendations, the group already identified that for those purposes where just contact needed to be established with a registrant, the registrant must provide an e-mail address or a webform to facilitate such communication. Again, there were a number of third-party purposes identified that focused on establishing contacts, so from our perspective, that seems to be already covered through that recommendation.

And again, this of course is a starting point for the group's deliberation. It's up to you to review this list and identify whether it captured the correct third-party purposes, if there's anything missing, and again, having said that as well of course, we didn't make any kind of determination [whether] any of these would provide or would rise to the level of [inaudible] providing that disclosure. This is just indeed a list of reasons or legitimate interests that we could identify from which certain user groups might request access.

We've also already made a next step, and we'll just scroll to the next page to kind of t urn it into a [inaudible] template, to support [inaudible] from the third-party purpose, we hope then to further [drill down] and identify the user groups and user characteristics that might pursue such a purpose, and the lawful basis for requesting disclosure, what are the data elements that are typically necessary for fulfilling that third-party purpose, and then already moving slightly into our next topic of conversation, the accreditation of other such user groups and authentication of such user groups.

And I know that there were already some conversations based on whether the starting point should be the ICANN purposes that were developed in phase one of this work, and [inaudible] from staff perspective, I think we're kind of aligned or at least our approach here was aligned with what Volker and Alan Woods shared on the list, that the purposes developed in the phase one of the group's work was to be focused on the collection of registration data. This is really about third-party legitimate interest to request disclosure of that data, and of course, although the GDPR indicates that those legitimate interests or third-party purposes should be incompatible with the purposes for

which the data was originally collected, that does not however that they need to be identical or at least that is our understanding. Again, of course, that's something the group can further consider.

So again, this is where we started. I'll just scroll back up on the list, I think from a [staff] perspective would be helpful to hear from the group if this approach is what you had in mind when you discussed last week and provided your input on focusing on third-party purposes. And again, one thing we may want to consider as well, the term "purposes" may not be the right one, and we've kind of reframed it in this way because the charter questions refer to purposes for third parties, and again, I think you all know that the charter was of course developed quite a while ago and before we went through all the deliberations we'd had to date. So one thing the group may want to consider is [inaudible] using a different terminology here. I think maybe third-party legitimate interest is one that has been referred to, and of course, we can then have a footnote to explain that although the charter question is referring to purposes. The group wanted to distinguish from purposes identified in the phase one, the ICANN purposes from the work that's being done here, so that may be something to consider. And [inaudible] question we're looking at the list, did we capture broadly the third-party purposes that had been described or had been flagged over the last months for why a third party may request disclosure of data? And I think also, again, your input on the approach and the template would be helpful, because one of the things staff struggled with, and I think those of you that have been on the RDS PDP working group may recall as well that we went [inaudible] back and forth on where to start. Do you start with the users, purposes or data elements? They're all of

course at the end of the day interlinked, so we do anticipate that it will be an iterative process, and we're having a template that touches upon the questions that need to be answered at the same time may help to facilitate the group's deliberations. I think I'll leave it at that and hand it back to you, Janis.

JANIS KARKLINS: Thank you, Marika. I see a number of hands up. Before giving floor for the comments, I think also, we should understand that if we want to progress, then we need to be as cooperative as we can, and I was following the comments in the chat room while Marika was presenting, and there were some rather negative reactions immediately when Marika started to speak. And my question is, why now? Why not two days ago when the document was posted and all of us had a chance to read it?

We tried last time one way to address issues through identifying groups of requesters. That was turned down suggesting we need to start with the purposes. Now there's a compiled list of purposes, now it's not anymore good. Now we need to start with something else.

So I think with this attitude, we will not get overly far. Ultimately, as Marika said, everything will be interlinked. We're talking about kind of a matrix, and we can take three-dimensional matrix and we can take either XA or XB or AC, and then start developing that matrix from one of three axes, and this is our choice.

So with these words, I would like now to see who is first, and that is Margie, please, followed by Alan.

MARGIE MILAM: Hi. Thank you. Thank you, Marika and staff, for pulling this together. I think focusing on purposes is the right way to go, and I guess my question for you is, are you now looking or actual comments on each of the categories, or are you just asking for input on the form and the process? And if it's just the form and the process, I think this makes sense. It's consistent with our charter, and it's consistent with GDPR since we'll need to be able to tell registrants how their data is being used and for what purposes. So I think this is a good approach.

JANIS KARKLINS: Thank you, Margie. Alan.

ALAN WOODS: Thank you. I suppose I have one or two queries specifically with regards to the way that the document is. I understand we're trying to [find a new way] of approaching this, but as I alluded to in my e-mail earlier, I do think [inaudible] approach of user groups is we're never going to be able to [inaudible] user groups, and what we're doing here is possibly creating instances where people may feel or believe that they have a legitimate purpose in order to request [inaudible] in the instance of the specific request, they do not have that legitimate purpose, because when you look a the actual request itself, it is not fulfilled.

So we have to be very clear. We're walking a very fine line about creating legitimate purposes. [inaudible] legitimate purpose is based on the actual content of the request itself, not about who has asked for the

data in the first place. So I would be cautious. I would advise caution on that.

The other thing that kind of strikes me as well in this is where we're talking about the types of particular data elements that might likely be included. Again, I would ask people to shy away from that particular concept as well, because in the request itself is the request for the data elements. Each request is not going to be, "I made a request, I'm from this particular user group, therefore you must give me everything from A to Z." Not at all. The request and the legitimate purpose of that request, and everything within that request, is based on what is being requested for what purposes, and indeed, [inaudible] establish the legal basis for each data element, not a swath of data elements in that particular case. So again, I would ask us to exercise caution on that one. I know we have to start somewhere, but let's start making this a proper and GDPR or just general data protection principle facing process. Thank you.

JANIS KARKLINS: Thank you, Alan. Hadia, please.

HADIA ELMINIAWI: So first of all, I did post an e-mail referring to some thoughts about this matter, but first of all, I want to say that for sure, the purposes of third parties are different than ICANN purposes, and definitely, third parties will need their own purposes for legitimate lawful disclosure.

My actual thought was with regard to the approach on the starting point through which we are [inaudible] approach which we started. We actually relied on the data that was collected in 2017 in relation to the retired WHOIS system, and prior to the GDPR and the temp spec. And this data in all cases was based on ICANN policies and purposes. So my thought was, why would we rely on this data? Why not have our starting point? The ICANN policies that we developed in phase one. Why start from ground zero?

Okay, what we're doing now might work well, but there's a problem. We shall need always to go back to the purpose that we put, because article 5(1)(b) of the GDPR, purpose limitation, says that the data needs to be collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with those purposes.

Well, disclosure is a form of processing for sure, and so even after we adopt this approach and rely on this data, after we finish our work, we will have to go back to our purposes and make sure that they are compatible with the purposes that we have put. And that does not mean I'm saying that I'm confusing third parties' purposes with ICANN purposes. No, I'm not saying that.

So that's why initially, I thought that our starting point or the base on which we should rely on should be our previous work in phase one. However, if the group feels comfortable going ahead with this approach, having the base of our work, the data previously collected, and starting from there, I'm fine with that as well, but I'm afraid that that will lead us later to problems related to compliance or maybe incompatibility with previous recommendations or work.

I'm fine going ahead this way, and let's hope that it doesn't lead us later to any kind of problems. Thank you.

JANIS KARKLINS: Thank you, Hadia, for your flexibility. And certainly, we will be attentive. The list which is on the screen now is just initial proposal, which may be – and certainly will be – edited in many ways, and maybe some additional things will be added, some things may be taken out or rephrased.

Milton, please.

MILTON MUELLER: Thanks. So, first, apologies a bit for reacting so strongly to the first pass at this. I realize looking back on the records that we were sloppy with our language last meeting. We did say third-party legitimate purposes when we should have said third-party legitimate interest, and probably this misled the staff in terms of what we were looking for, but it really is the legal standard that we have to be looking for and not purposes. And I really got freaked out when she referred back to the RDS process which I just have a lot of unpleasant experiences with.

So we do need to talk about third-party legitimate interests and other specific legal bases, Brian, which are not purposes, and I'm sure Brian would agree with that. And then I want to go back to what Alan said, which was very hard to hear from where I am, but I think if he's making the point I thought I hear, it makes our task a little more complicated, which is it's not just that you can say in some abstract sense that, yeah,

prima facie, this looks like a legitimate third-party interest or some other legal basis, but we have to look at the specific disclosure, a specific request for specific data elements.

For example, it's perfectly possible – I suppose for the sake of argument – and I would not recommend this – as an academic researcher, we said that academic research could be a legitimate third-party interest.

Now, number one, you have a problem of people disguising themselves as academics in order to get data that they really would use for a different reason, and secondly, you have the issue of, what exactly is it that justifies this particular academic research? Is it asking for too much? Is it asking the right amount of data to be disclosed? What about anonymization, those kinds of things?

So I hope nobody thinks that if we have a list of things that we, in the abstract sense, consider to be legitimate third-party interests, that that sort of solves the issue and somebody can just come up and say, "Oh, I correspond to category B and therefore give me whatever I want, no questions asked." Thank you.

JANIS KARKLINS: Thank you, Milton. Alex.

ALEX DEACON: Thanks, Janis. I kind of feel like we're a dog chasing its tail here. All of our discussions seems to just go in circles, and I have a fantasy that one day we'll start to actually have real discussions around the charter

questions. If you look at the charter questions, I think they do a pretty good job of getting us to where we need to be eventually. Question A1 talks about what are the legitimate purposes for third-party access to registration data?

We could debate the terminology there, but it's in the charter and I think that the document that staff put together puts us on the right path to have that debate. We shouldn't we shouldn't get wrapped up around other important details because they will be addressed in discussions we will have later on. Again, if we if we just work down the charter questions, we will eventually talk about the legal basis to support the purposes that we will soon define, and then we will at some point talk about eligibility criteria.

And then once again, at some point, define these groups, and then A5 talks about once we've done that, what element should each user party have access to based on the purposes? So I suggest, if possible, that we stick to at least a framework of the charter, focus on the specifics of each charter question for now without getting into the details of the discussions that will happen later, and if we do the right thing in an organized way, then I think we'll end up at the end with a policy that will define how this data can be made available to third parties.

So just to summarize, I think this document is a good first start, and I suggest we try hard to focus on the task at hand without getting into the details of discussions that we will have, definitely have, important discussion that we'll definitely have at some point in the future. Thanks.

JANIS KARKLINS: Thank you, Alex. If I may ask other speakers now to concentrate on the list of what is now on the screen, of the legitimate interests and requesting the disclosure of registration data by third parties. Milton, I think that this is your old hand, and I'm taking now Alan. Please, Alan Woods.

ALAN WOODS: Thank you, and I changed microphones, so hopefully it's a bit better for people.

JANIS KARKLINS: It is better.

ALAN WOODS: Excellent. Great. I'm noting what you just said there as well, Janis, I just want to be clear. I just think that number one, with what Hadia said, let's just be clear that what she stated quite clearly was third-party purposes, and we do not need to share a purpose n order to disclose it. And this is, again – and I will be very brief on this – why I have an issue. An ice cream vendor can ask a registrar, a registry or whoever for disclosure of details for any purposes that could potentially be out there, and if it is legitimate in the interest of that particular ice cream vendor, then we will give it. That's why I think starting with this is giving a perception of people who are on this list who have this particular purpose will get an automatic buy into the next round, and I just want to be sure that we know that that is not the way that this law works.

So I just want to put that on the record, and I think actually Thomas potentially had a good idea. Maybe we should just talk through a scenario and see where it goes, and maybe we'll show the issues. But I do think that there's probably an underlying basis that we need the legal team to go through and get a few answers to some very tough legal questions before we can actually figure this out. Sorry. Thank you.

JANIS KARKLINS: Thank you, Alan. My idea for this meeting was to collect general comments on the list of purposes and then to see whether the table, which is on the second page, is something that we could prepare for each of the purposes as we advance in our conversation.

Volker, please you are next.

VOLKER GREIMANN: Yes. Two points. The first point is to Hadia's point that if the data was not collected for a certain purpose, it cannot be used in any other way. that's not quite correct, because the purposes under the GDPR article [6.1.] are quite ,and open, for example if there's a legal obligation to do something, I may still divulge that information for example being part of a subpoena or other legal obligations, [I might face] court orders that force me to divulge [inaudible] even if I never collected it for that purpose. So there are ways around the disclosure of collection purposes, and allowing for a broader disclosure purpose.

And the other thing is I don't think we need to be all encompassing with our user groups, because we may have to decide at a certain point that

there are user groups that may have legitimate interest but we do not want to cater to them. As Alan said, the ice cream truck may have a legitimate purpose to request disclosure, but being a small group or a fraction group, they will have to resort through legal means, not avail themselves of the disclosure framework that we are designing.

So we might want to exclude certain groups from our disclosure framework because they have other ways of getting at the information, simply because going into detail too much might just take forever. Thank you.

JANIS KARKLINS: Thank you, Volker. I think Ashley made a good comment on the chat which we may want to think even endorsing, and I quote her designation of a group and [number] of the group does not assume that access or disclosure will be granted. So that is obviously the general framework or general understanding that we should have. Alan, then Stephanie, and Thomas. Alan, please go ahead.

ALAN GREENBERG: Thank you very much. I originally put up my hand to comment on Alan Woods' original common and Milton's but I think Volker hit on something that I think is really important. Our presumption in going into this whole exercise is not that every request is going to be handled on an automatic basis and because you're a part of a group or because it's a certain class of request, it's going to be satisfied.

The presumption is that some classes of requests and types of requests from some groups of people who are members of groups and are appropriately authenticated will be easy ones and won't necessarily require detailed human review to look at all the details. A UDRP case perhaps.

And our assumption is there's going to be large numbers of those. That's why we're going through this exercise, there's always going to be requests from any class any group of people and any class of person that that are not going to fall into that category. Academic research as Milton's example is a perfect one. They're going to be so varied that they're going to require – and perhaps require so much data that they're going to require the manual intervention and certainly a lot of care in responding to them, but our assumption is that there are going to be certain ones which are going to be a lot easier to handle. And those are the ones that we need to actually start discussing and get down to the work and try to find out, are there ones like that that we can identify? And the edge cases will always be there, and let's not focus on the edge cases right now, acknowledging that they will be there, but those aren't our problem today. Thank you very much.

JANIS KARKLINS: Thank you, Alan. This was exactly the reason why we as example put first the law enforcement table on the second page, because that is probably the most straight forward and mainstream case that we need to start talking about and then develop our common understanding around this case and then see what we can do with others.

Stephanie, please.

TERRI AGNEW: Stephanie, you may need to double unmute.

STEPHANIE PERRIN: Thank you very much. I have a bit of a problem In that I continue to lose the screen where the unmute button is. As I said earlier in the chat, I think the computer and I need to take this course on Zoom. It disappears and I can't get it back.

I was going to endorse actually rather the reverse of what Alan said, although I want to endorse his common-sense approach to this problem. There are certainly large groups of types of requests that we need to figure out how to facilitate. The unfortunate thing and why we're protesting so much about sorting on purposes is that it doesn't actually help us figure out the modalities of how we're going to approve requests or not. And I know that we're holding up Steve who's ready to tell us about the system he's designing. There are certain things that can be done, and law enforcement is one of the easier types of requests, that's why it's in a separate category under GDPR. Third-party requests will not be treated, if we're going to follow the law, the same way they've been treated until WHOIS in the past where the policy just said these are legitimate, you will make all this information available for them. You are still going to have to discriminate on each case.

Now, the edge cases are instructive and a lot of the bulk requests we've had in the past are going to turn into edge cases. So I think it's quite

useful to go through the ice cream truck type of scenario. And I would just like to reiterate, at the risk of seeming like a real pedant, as I always do, this may be new to ICANN, but it is not new to everybody who's been dealing with the access requests from third parties in data protection regimes around the world for the past 30 years.

So there's a lot of experience in coming up with procedures and forms of what you need to ask for before you agree to the ice cream truck requests, the Stephanie Perrin filing a competition act complaint, the Milton Mueller looking for research data. They're all different, but you can still develop procedures for them. But they those procedures are not based on purpose. They're based on legitimate interest. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Indeed, the edge cases will probably keep us busy, but maybe we should start by working on mainstream cases that we have a basis to address also those edge cases and fine tune our system. Thomas is the next.

THOMAS RICKERT: Thanks very much, Janis, and I think that we're now moving the discussion into very constructive direction, so we seem to be willing as a group to start with one scenario, purpose, or whatever you might want to call it. I would prefer not to use any legal term at this stage but just talk about things that happen in real life. And we just need to pick one scenario that occurs that we can use as a test case for going through, describing what the requirements are, then looking at the legal basis for potential disclosure and looking at ways of maybe standardizing such

process and making it fit under an accreditation system of whatever shape or form, of which we don't know at the moment whether we can do it.

I do understand that the idea of starting with law enforcement requests is intriguing because we have a public authority that enjoys a lot of respect and there are checks and balances in most countries around the world. But the issue with that is that GDPR has a specialty when it comes to public authorities and data processing, namely that they can't claim to have a legitimate interest for data processing under 6.(1)(f). So we would need to look at legal bases for law enforcement authorities for individual countries based on 6(1)(c). The disclosure request can then potentially be honored. And I think that will probably take us down a rabbit hole.

So my suggestion, which I hope you will honor as constructive, would be let's just look at a scenario that contracting parties are facing every day. There is a company that owns trademarks and they're seeing cybersquatters registering domain names that either are identical or resemble the strings that they enjoy protection for.

Don't scream they should be going to UDRP or URS immediately. Let's just play this through. What do we need for honoring such disclosure requests? I'm not going to do it now, but I would really like to start with such a scenario, because number one, it will help us build on what we've designed for individual disclosure requests in phase one, so we have something to build on in our report, and GDPR also allows for data processing when it comes to civil claims. So we have some something to

lean on and we don't have to enter too much uncharted territory when we're looking at such scenario.

And once we write that up and go through it, then we can potentially use that as a straw man, although in the ICANN world, probably, I should use the word strawman because it's encumbered with some ministry, but we could probably use that as a strawperson to then replicate for other request for disclosure scenarios. That's my five cents. Thank you.

JANIS KARKLINS: Actually, that was dollar. Can I ask you one thing? Would you be willing to make a write-up for that case that you just suggested for our next meeting or meeting after that we could go through and play through this case, which you said that everyone is facing almost daily? And that may be then on the basis of the table which is on the second page, we could maybe agree to use that table as a template for every case we're discussing and working on. Thomas, I see that you're volunteering, your hand is up.

THOMAS RICKERT: I didn't only raise my hand to volunteer but also to ask you as chair to kindly test what the group – whether there's any opposition to taking that approach, because we've tested two different things, and I'm very grateful that you and staff took it upon them to write documents in the hopes that the group would like them. So I'm happy to write something up, but let's test whether there's a position to pursue that approach. And if there's no opposition, then I think we should just take the chance

and try to work through it, and if it works, we can all move on to the next scenario. If it doesn't, you have to blame it on me. Thanks.

JANIS KARKLINS: No. For me, your proposal [inaudible] intellectual property-infringement, and that may be only one of the cases in preventing intellectual property infringement. But we could see several of them, and once we will be working, we would get kind of in the rhythm, and then probably we will advance in putting those building blocks together.

So the question is, would the team be in a position to agree that Thomas would do one write-up for our consideration for the next or one after meeting on the intellectual property infringement, the case that he just described? Any opposition? I see none. Thank you.

Thomas, you have homework. Marc is not willing to speak, so Thomas, you have homework. If you need staff support, please contact Marika and see whether any staff time is available to assist you in your exercise.

So since time is flying, we should maybe listen now presentation of Steve on his work. Let me maybe suggest the following: please look to the list of purposes and please feel free, edit them in every possible way you think appropriate. Please think of any other purpose you can think of or subpurposes if you wish, like Thomas' case on a typical infringement of intellectual property or anything else. And please, do it throughout this week until next Tuesday that we could compile and then bring the updated or edited list to the next meeting. Also, I would like to ask to consider proposed example of law enforcement and provide maybe general input since we did not have chance to talk it

through, and we would take it the next meeting. Would that be acceptable? I see no objections.

Now I will move to next agenda item, and that is presentation of Steve Crocker on behalf of Barbecue group. Steve.

STEVE CROCKER: Thank you, Janis.

JANIS KARKLINS: Welcome, and now microphone is yours.

STEVE CROCKER: I have a presentation that I'd like to share. Let's see. Am I allowed to do that?

TERRI AGNEW: Hi, Steve. You sure are. Go ahead and just select the "share" option in the middle."

JANIS KARKLINS: We see your slides.

STEVE CROCKER: Okay. Now let me put it in presentation mode, and I will talk for a minute or two before I get going. So I've been watching the endless WHOIS issues for a long time, I don't mean years, I mean decades. And

one of the things that I continued to think about after I stepped off the board was that it would help a lot, I think, to have some precision in the discussions that go on. I have to express quite a bit of empathy for the discussions, and I just listened to the last roughly half hour. You guys are wrestling with precisely the hard problems.

And I'm not here to offer a solution per se, but we're building tools that we think might be helpful. So with that, just describe what we're doing. Even before I left the board, but certainly while I was on the board, put a lot of energy into this area. I felt that it was useful, maybe necessary, to do a much deeper dive into the fundamentals. After I left the board I continued to think about it and I was fortunate enough to be able to assemble a small team of people who felt similarly who were expert, very knowledgeable. And in a kind of fashion that's more like the IETF and less like ICANN, we organized ourselves into an informal group operating quietly, without charter, without authority, and without any funding, actually.

And these people, most of whom you would recognize quickly, asked that their names not be visible, at least at this point, so as not to implicate their organizations, although their organizations do know and fully support their participation. So we've adopted this quirky name of the Barbecue group which is a quirky play on French mathematicians of last century who adopted a cover name after a French general, Bourbaki.

Whatever results from our work is going to have to stand on its merits instead of because of any authority or pressure from the fact that we're the people who said so.

So with that, let me take you down – oh, the other caveat is at this particular moment, I've just been coming through a perfect storm. We did a lot of work, we built a framework, began to test it, and discovered that key parts of it were working well and a key part of it was not working well, and the key part that's not working well is precisely in the area that you're working on.

The other part of the perfect storm is that I've been ill for the past couple of weeks, and although I've been working feverishly to do the revision and take a revised approach to the access policies, I'm at a moment of maximum disarray.

So with that as a sort of caveat and slight apology, I'll now take you through where we are, and looking very much to interacting Q&A as we get through this.

For those of you who have seen the previous – several of you have seen the previous version of this, you will see that that a large portion of it has been sort of ripped apart, and then that's it, not yet put back together again.

Okay, so there were no surprises here except that down at the bottom, the basic tensions over time have been privacy versus accuracy versus effectiveness of the whole system, and in my estimation, there's been a general assumption that you can't have all three of these, that they trade off against each other. I think it's possible to have a positive sum outcome here where there's an improvement along all dimensions.

GDPR in my view has been like throwing dynamite into a log jam. It's forced the attention to privacy, broken the log jam, but it's otherwise a

fairly blunt instrument, doesn't provide detailed guidance. That's what we're all struggling with. But GDPR is just one force to reckon with in the world. There's privacy issues cropping up everywhere from California to Asia, and so forth, so taking a somewhat broader look.

And by broader look up, we're looking at all of the information is collected, generated under all policies, both policies that are in place and policies that are being proposed. And when I say all information, I'm talking about a very wide spectrum from the stuff that is obviously publicly available, DNS records, to stuff that is obviously very sensitive like credit card details and account passwords and so forth.

And implicit in all of this is that there should be a justification for each piece of information that's collected. This is bread and butter for all of you and doesn't need to be said. But I do want to say that our perspective is that we're looking at crossing both the G and CC space, not just limited to one or the other. So the ICANN contract which obviously is very important for us but only covers about half of the world.

So the project we worked on this is we've been developing a candidate framework that reflects what we've heard. We've iterated several times at quite granular, and the last sub bullet there says initial framework waiting for testing. Well, we took it out and tested it some and got some very positive feedback, but also discovered that, as I said, the access side is going to need some larger work.

So we're currently – I'm wondering if I've got the right presentation here. With apologies, I need to check. Shoot, this is another part of the perfect storm about systems not working at the right time.

Alright, so Just another set of general principles here. This is not intended as [inaudible] it's not intended as a political exercise. This is intended to be descriptive not prescriptive. It's more a question of capturing what ideas are floating around, tearing them apart and putting them back together. So it's a fairly analytic and synthetic approach not intended to drive in a particular direction, but to highlight in a somewhat fine-grained way those things that we can systematized but also of course leave room for things that we can't systematize.

So here's the revision to that project slide that I had intended. We're now in a phase of doing the revision based upon the early feedback and I have a very twitchy little mouse here. We haven't tried to go public in the sense of unveiling this for general use. We have had a few dozen interactions, including with several of you, but other groups as well trying to gather as much data as we can, work closely with people who are thoughtful and not try to make a big splash, at least not yet. When we are ready, we will make available the instruments that we are preparing and try to see if that will be useful to people to use both internally within their organizations and to exchange information and to do analysis with.

Here's a somewhat messy slide that is not the best, but try to represent the following idea, that you have both policy flows and data flows and the policy flows typically from various authorities to registries and registrars and to registrants, and you have data flows from the

registrants back the other direction through various registrars and this probably should be continued back into various registries, and then you have requests from various requesters. And symbolized here, not very well, are the fact that there's gonna be some policy issues exactly related to the discussions that you guys are having, which ones are automatic, which ones have to be dealt with manually, what are the bases, how do you compare them, and so forth. And that's an area that we're working on.

Let me introduce the notion of policies versus policy sets. So when somebody registers for a domain, a bunch of information is requested and a bunch of options are given. We're calling that the policy that the registrant sees as presented by the registrar. Now, what that policy is is governed by a series of external forces along the lines that I've described in this slide here, and some of it may be determined by the registrar but much of it will be determined by the authorities that it reports to.

For example here, I've shown that dot-com and dot-info are subject to both ICANN and GDPR. Dot-cn maybe less so, but governed by national government and so forth. So the actual policy as developed and an executed by the registrar may have multiple overhanging authorities that it has to deal with. So, the representation of those overhanging authorities – apologize for the word, not the best – is that they specify a range of possible policies, permitted policies, or to use a slightly different term, a set of policies.

Let me motivate it a little bit. These things will not have a lot of – are not super compelling from perhaps your point of view because they

may seem obvious, but registrars collect a lot of data that they use internally and don't pass along to the registry. What is the registry's policy with respect to that data? Well, basically it says "We don't care." Registries may or may not leave it up to the registrar whether to verify specific pieces of contact data. If they leave it up to the registrar, the registrar may decide that they'd want to verify the contact data or they may not.

So there's latitude usually of various sorts in the perspective from the higher authorities and then you have a question. When you have multiple higher authorities that you have to be consistent with, can you compare how they would be related to each other?

What we have been able to develop is that with an explicit representation of the policy sets and policies, it's easy to see if they're consistent and doesn't tell you how to resolve in consistencies but it points out where they inconsistencies are and then brings that to the surface for discussion. I'm happy to take questions along the way, or not. What's your preference?

JANIS KARKLINS: Steve, I think you better go through the whole presentation, and then we will open Q&A.

STEVE CROCKER: Great. So under collection and disclosure, the collection side of this is what data do you collect starts with a dictionary of data elements. It needs necessarily to include all of the things that for example are in

your phase one report, but likely includes other things that may not be in the phase one report but are part of what the daily discourse is between registrants and registrars. And then what the purpose is of each data element.

The policy is whether collection of that data element is required, optional or forbidden and whether or not verification is required. On the disclosure side, this is the part that we're replumbing, and a piece of insight that I don't know exactly whether it's accurate or not, and I sort of want to be clear about, is that typically, my understanding is that if you ask for the record related to a particular domain for example, the collecting organization will basically give you the whole thing or not.

That's not quite true. They obviously will give you if you're asking a public question, they'll give you the public part. And if you're asking if you have higher authority, they'll give you more, and if you're a law enforcement they may give you even more. So this is an area where we're trying to see how much variation actually exists and what the structure of that variation is. The obvious extremes are the lowest would be public access and the highest would be for law enforcement, but there's obviously intermediate things. And the question is, is every one of the requests that is in between law enforcement and public ad hoc and distinct, or do they fall into groups? And as [I] say, that is something that we're trying to figure out.

We know, for example, that there may be different policies for natural versus legal persons. We also have learned that it's becoming common as the policies swing toward the privacy side that registrants are asking for and are getting in some cases the permission to say, "Thank you very

much for protecting me, but I want this part of my record to be public." So there's a question of whether the registrar permits the registrant to downgrade the sensitivity.

Why two sensitivity levels? Puzzling about what is meant by redacted. In the wider scope view that we have, there's an awful lot of data which is not available and not even acknowledged, so it's not just a question whether information is public or redacted. There's got to be at least three levels: public, redacted and above that level where it's not mentioned. So as we're modeling that, suggesting here to sensitivity levels. And I apologize for the sort of math oriented version of this, but a disclosure level where the lowest of which would be public, an acknowledgement level, which is If the disclosure level is public, it doesn't matter, but if they disclose your level is above public, then acknowledgement level is what happens if you don't have the right to see the data, do you have the right to know that it's there?

So that leads you to three cases: a request has a sensitivity level. If that sensitivity levels above the disclosure level, then you get the data. If the disclosure level is not above the disclosure level, but it's the public acknowledgement level, then you get the notice that it's there and you can't see it, which has been commonly called "redacted." And if the request level is below the level of acknowledgement, then you don't know anything. You don't get anything, and that's the way it is.

Alright, now a framework where we have a revision in progress. This is the main portion of a spreadsheet which is intended to integrate all of this. This is the 100,000-foot level, you're not going to be able to read this very much, but I want to give you the main pieces of it. Here's the

list of the data elements, here's the collection and disclosure policy. The distinction between the blue and the green is that the green is the policy of this particular organization. So think of this as the policy that a registrar has.

The blue is the cumulative effect of a series of higher order authorities, and the intention is that we should be able to take a separate spreadsheet for each one of these authorities, lay out what its policy is, and then clash them all together and show what their effect is so that you can then see whether or not this particular policy of this registrar is consistent with these. And the same thing actually works at a higher level of seeing whether or not the collection disclosure policies of the higher authorities are consistent with each other. You could imagine a situation in which two authorities are specific about what they want and those and those specifics do not match up with each other so that nobody could satisfy both of them. So this would be a way of highlighting that.

When we reassemble this, the white part here is a illustrative set of registrations. And then here's a request, and based upon what's in this request, you would get different responses and be able to see what that is. Here's a slightly larger view of what the data elements look like, various contacts. One point that perhaps treads into the policy area, but it seems to me that by specifying what's expected of each contact, what their authority and responsibility is, that that would go a long way towards sorting out some of the ambiguities.

The admin and tech contact as we know predate the existence of the domain name system, predate the existence of the Internet, they go all

the way back to the ARPANET and were published so that the system administrators could find each other and help sort out problems. That's been carried forward with no hard definition as to what those roles are or what those people's responsibilities are. That's certainly something that could be addressed along the way.

So that's one group of things. Another thing which I've always found odd is that the account holder, who is distinct from the registrant, is the one who has the direct relationship with the registrar. He's got the keys to the kingdom. He's got the password and account and can change records, more or less within seconds, and yet does not get mentioned in any of the policy issues.

So again, this is another case of bringing things to the surface. What you can say about the account holder, of course, is that the registrar knows who the account holder is. That information is typically not passed back to the registry for thick registries, or otherwise made available, but nonetheless, say your law enforcement person may be extremely interested. Here's the DNS records up here. [Here's] various operational issues, some of which might be sensitive and some of which might not be. Payment details, obviously very sensitive. Registrar ID, probably public. Other details about when it expires and the registrant is maybe more sensitive.

Over here on the collection side, this is a quick sketch of a part of what this will look like. I've got some construction to do and then I have some cleaning up to do, but it's along the lines of what I said. And we can come back to that. Here's some other ideas that have been discussed

but not pursued, but we're cognizant that these might become important in the scheme of things.

The desired outcome for the project is a useful tool for expressing and comparing policies, hopefully to stimulate discussion on what data should be collected, why, who will use the data, etc. All of the things that you are all concerned with. Looking beyond the current efforts of it, there's been a long-standing view that from the point of view of the people operating the WHOIS systems that it's a [drain] and viewed as a negative, but I think that's not the optimum view. The registration data directory service also have some potential positive. It's an important point of coordination.

One area, just to flesh that out a little bit, is the DNS operators have no pathway for updating the DNS SEC records to the registry, because they work for the registrant, and the registrar owns the relationship with the registry, at least in the ICANN world, and if you just take the text as written, only talks to the registrant. So when the DNS operator has to update the DS record, there's no way to get that there. So that's leading to a lot of workarounds and so forth.

It's a bit of a distraction for this discussion, but I'd just give you an idea of the things that we're thinking about. And that's the condensed version of where we are. Time to open up for discussion.

JANIS KARKLINS: Thank you, Steve. Now we have a chance to ask questions to Steve. Who will start?

STEVE CROCKER: I've left you speechless.

JANIS KARKLINS: No, there are a few. Alan is first, Alan Greenberg will follow.

AMR ELSADR: Thanks, Janis, and thanks, Steve. Steve, you had mentioned sensitive data and sensitive requests, or the sensitivity level of data and the sensitivity level of requests in an earlier slide. Sensitive data to me – because you mentioned credit card payment details as an example – I've always assumed that when we refer to sensitive data, it refers to the special categories of data that are mentioned in the GDPR in several recitals as well as an article. I don't recall which one it was. But I didn't see much by way of explanation of what sensitivity level of requests means. If you could shed some more light on that and also explain what the implications of the different sensitivity levels of these requests are, I'd appreciate it. Thank you.

STEVE CROCKER: Sure. Again, I have to frame this as kind of grappling with how different parties view things and how best to represent it. People don't seem to explicitly think in these terms, but the question is whether or not we are intuiting properly that that's underneath what's really going on. So I think about the registrar collects all this information and then somebody asks for the record. Well, what they get it depends of course on who they are and what they're asking for.

Requests typically – and I'm more than willing to be told that I'm quite wrong about this, that the requests aren't down at the level of "I want this data element, but not this data, I want this data but not this data" and basically say, "Please give me all the stuff that I can have based on who I am and what I'm asking for." So if you're a member of the general public, then you get a certain layer of information. I'm using the word "layer" deliberately. And if you are somebody with credentials or privileges or authority – and I'm lumping all those ideas together – you'll get more information. So you can think of this as a coloring, if you will, the totality of the information that the registrar has and the base color is called public, and there may be other colors. Now, how many there are, how common that is, how useful that is across the spectrum, I don't yet know, but starting with the hypothesis that there's only likely to be a few different colors, if you will, and it's easy to expand and it's easy to see that in the extreme, it could get out of control, but it's also not unreasonable that similar decisions about how sensitive something is or what would be available made available to one group or another would be common.

If that's too abstract, let me make a guess. And this is just a guess. So you've got the DNS records, clearly public. Let's say registrant contact information is obviously more sensitive, and even if you divide that up into the registrant's name versus their home address, you're going to wind up with a couple of different levels of sensitivity. How much variation is there in all of that, as I said, we have to see, but I'm guessing that this shakes out into a fairly modest thing, otherwise it becomes very complex.

Now, the other half of the question is, well, who gets to see that, and who determines what their authority is or what their privilege is? That is not something that will be determined within this framework. What will be determined in this framework is a way of specifying what the answer to that question, is and then focusing on the decision processes associated with that. Some of those decision processes will be automatic. Some of them will require judgment, manual processing, and some of them, it may be possible to say, "Hell no, we know who you are and you can't have what you're asking form," and thereby sort of triage the whole situation. Does that help at all?

JANIS KARKLINS: Let's see.

AMR ELSADR: [inaudible]?

JANIS KARKLINS: Clarifying question?

AMR ELSADR: Yeah, could I just follow up?

JANIS KARKLINS: Please go ahead.

AMR ELSADR:	Thanks, Steve. I'm not really sure that I did get a clear idea of what sensitivity level of requests are. But going through this whole process, especially our work on phase one, I think there a lot more to processing requests for data disclosure than just who the requestor is and what data they're requiring.
	I'm sure you've been following our work very closely, and as you know, there's a lot more involved than that. The legitimate interests, the legal bases for the requests, as well as notifying a registrant or a data subject in advance that these are the identified purposes for which their data will be processed. And from what I gathered from your answer specifically on the part regarding the different sensitivity levels for requests, it seems like, again, those depend on the sensitivity level of the data. Did I get that correctly? Depending on a requestor who's asking for a specific set of data, depending on the sensitivity level of that data that determines the sensitivity level of the request itself? Did I get that right?
STEVE CROCKER:	More or less. These things are intertwined. We started down the path that a particular request would have a very detailed list of data elements are asked for and what data elements are not asked for. And I discovered for various reasons that that's very unwieldy and very unlikely. You can imagine the steady state in which the quests are well defined and the authorities are well defined and so forth. But in a dynamic system, starting from scratch and adding things and changes over time does not really scale and requires an extraordinary amount of centralized control.

So, the question is how to put together a system that can evolve from where things are to maybe some more mature state and also accommodate changes over time. So, as I said, my current thinking is that it seems unlikely that requests from different parties are going to be at the level of listing every element in the data dictionary and saying, well, we want this, and we don't want that. And we want that, and so forth, and more likely to say "We'd like sort of as much as we can get related to the following idea, "and a question that yet to be validated is whether or not that can be encapsulated in the sensitivity levels or sensitivity labels that doesn't have to be purely hierarchical, and see where that goes

And then going back to a comment I made at the beginning, having discovered that the original idea didn't work, we're now in the process of ripping them apart and putting together a next version of that. I don't have the pieces of that quite working, and it will not surprise me if that too turns out to be a reasonable but not good enough guess.

JANIS KARKLINS: Thank you, Steve. I think we need to look to other questions. Alan, Kristina, and Mark SV.

MARGIE MILAM: Thank you very much. I'd like to thank Steve and the other anonymous people of this group for doing this. We have been in the situation for a long time where we we've never tried to group all the information in the same place to see whether it even makes sense. And the classic example, in my mind, is we require registrars to collect billing contacts.

They don't use it for billing, It's not published in the current WHOIS or the old WHOIS prior to GDPR. The only people who would ever see it are law enforcement if they use a subpoena or something like that to get the whole record, and yet we have continued to insist that registrars collect that information. So pulling it all together in the same place, and at least making these kind of relationships obvious, I think, is getting us farther on than we've ever been before. So I thank you for doing the work.

I tend to agree with you. That although we have a lot of data elements, we probably can group them together and simplify the overall picture in terms of disclosure and things like that remains to be seen, but I'm optimistic of that, and in fact the ALAC is currently discussing a suggestion that's akin to that. So thank you for the work and I look forward to seeing evolutions of it.

STEVE CROCKER: Thank you, Alan. And let me just make a – you reminded me an interaction. I've talked to a registrar that says "We don't use any of this data like billing contact. We know how to reach our customers. This whole thing is extraneous to us" So there is a discrepancy between the data that's collected under contract versus what the registrars actually use. And from a law enforcement point of view and preferably for others, they want the real data as opposed to the information that's forced to be collected, but which is not otherwise intimately related to the relationship. That's what leads to data being stale or incorrect.

If you like analogies, a single lens reflex camera gives you a picture through the same view that the picture will be taken and as was a major advance in photography. This is similar. If you want the data that is actually being used.

JANIS KARKLINS:　　　　　Thank you, Steve. Kristina.

KRISTINA ROSETTE:　　　　Thank you, Steve. This has been some very interesting food for thought. I had a couple of transparency-focused questions, one of which is a question that I would ask any expert that presents to us and one that is more specific to your presentation.

The general question – and I think you may have alluded to this answer in part. Can you tell us whether the work that you've presented is being funded in whole or in part by any third party or was started and is being conducted for the benefit of any third party?

STEVE CROCKER:　　　　　The funding comes from my children's inheritance and the benefit is for the Internet.

KRISTINA ROSETTE:　　　　Okay. Thank you.

STEVE CROCKER: Not a penny has moved anywhere. It's been primarily my time with the volunteer from others. I do want to say – not trying to be naïve about all this, I could imagine that if this requires more effort than I'm able to put in, and particularly as we get into actually providing an instrument that other people can use, that it may make sense to look for transforming this into some sort of funded effort, but the goal here is to be – except for the people I've mentioned who don't want to be transparent is to be completely transparent and not to be captured or working on behalf of any particular party.

KRISTINA ROSETTE: Okay. Thank you. I agree that's really important. The next question in your last comment is a good segue to this, is do you anticipate at any point that the other BBQ participants will disclose their identities? In other words, once the work gets to a final form, do you anticipate that would happen at any point?

STEVE CROCKER: It's not unreasonable. It's not something we've discussed. We've got our heads down focused on the technical stuff as opposed to political stuff. If one looks back at the analogy that I used, the Bourbaki group, most of the names if not all of the names of that group were eventually disclosed. And I don't think that the people involved in the Barbecue group would be unhappy if their names came to light. But as I said, it's just the courtesy of providing a quiet place to interact and they can, if they choose – there's no group rule or anything – individually to disclose their names, that's perfectly fine with me.

KRISTINA ROSETTE: Thank you so much.

JANIS KARKLINS: Thank you. We have four further requests for the floor, and we have about eight minutes remaining. Please keep that in mind. I have Mark, Georgios, Stephanie and James in line. Mark, please.

MARK SVANCAREK: Steve, I think there was a question early on from Amr that I'm not sure you completely answered. So in the phase one final report recommendation 18 we laid out a list of details that are required in order to make a data request. You have to say who you are and what processing you will perform, what is your legitimate interest, etc. and I think of that as a data payload. So here's my request, it contains this payload which has all these details, and those details would apply whether you're making the request by post or webform or e-mail or a theoretical automated system. And your system here would not preclude the delivery of that that payload during the requesting process, as I see it. It would just be assumed that you would be doing that and that the authorization would be based on that. Is that a correct assumption, or am I misunderstanding?

STEVE CROCKER: That's absolutely correct, and I thank you for elucidating that. It goes back to a comment at the very beginning. This is not intended to be a design that leads directly to an implementation. It's a conceptual

framework, and so the pathways for communicating could include exactly all of the things you said, anything from postal requests to an RDAP request or to a web-based request or whatever, and all of those are in some sense below the level of discourse that we're trying to focus on here, although there do have to be hooks, I do acknowledge that one wants to be able to distinguish between – so when you lay all that out, how much of this could be automated, how much requires special case handling, and so some of the discussion that I listened in to earlier in the call about edge cases versus core cases, become part of a broad view of a system, and then you can even look at quantification of how many of these things, how many requests of various kinds there might be, and what the cost of processing them might be and how many of them handle it automatically versus manually.

AMR ELSADR: Okay. Thanks for clarifying.

JANIS KARKLINS: Sorry, I lost everything that is on my screen. I probably need to leave and then come back. Who was next on the list? I don't see now.

GEORGIOS TSELENTIS: I think it was me.

JANIS KARKLINS: Yeah, please go ahead.

GEORGIOS TSELENTIS: Yes. Thank you very much, Steve, for this analytical view, and the Barbecue group for this analytical work. My questions refer to what you said about policies and legal frameworks that define how disclosure would be realized. Depends how [inaudible] the legal part on jurisdiction. You mentioned also about your model handling also ccTLDs and gTLDs. I'm interested to know how your model takes into consideration data flows or decisions that are crossing different jurisdictions, if you thought about this question. Thanks.,

STEVE CROCKER: Thank you. in some sense, we're looking at a kind of uniform picture of restaurants all over the world, registrars all over the world. Each registrar is responsible or in some sense controlled by one or more superior authorities. The point of view is, can we lay out what the policy sets are of each of those – let me put it more precise, can we provide a tool that allows each one of the policy authorities to say what its policy set is, and then a particular registrar or a particular registry can say, I am subject to the following list of higher authorities. Can I take the explicit representation of their policy sets, clash them all together so that I know what their constraints are that I have to conform to a whole want to be all of them and then see whether or not my policy set – if we're talking about a registry, or my policy if we're talking about a registrar, conforms to or is consistent with the constraints from those multiple authorities. So it's intended to apply equally, say, to a CCTV operating in Europe that is not subject to the ICANN rules, but is subject of course to GDPR and various national requirements.

JANIS KARKLINS: Thank you. Who was next? I still don't have a screen, sorry.

AMR ELSADR: I think Stephanie is next.

JANIS KARKLINS: Yes, Stephanie, please.

STEPHANIE PERRIN: Hi. Thanks very much, Steve. I just wanted to comment on this whole sensitivity thing, number one, ask you whether you did a data protection impact assessment, a DPIA, because that's kind of helpful when unpacking the sensitivity issues, and to comment on my own perception that we have a problem at ICANN dealing with the whole sensitivity issue because we don't collect the information, nor can we, I think, under the current rules that would allow us to determine whether disclosure was sensitive or not.

So first of all, number one, Farzaneh and I wrote to ICANN a while ago. I believe it was at Barcelona, saying that basically we were still violating data protection law. We were not popular, but you have demonstrated this, overcollection of data, i.e. the billing data, is classic overcollection, and if it's still around anywhere, even in escrow, you have to dump it. And we don't believe that this has happened yet.

Now, on the issue of sensitivity, we have gone on and on about the protection of individuals who are engaged in human rights activity, in journalism, in counseling women for abortion, in counseling LGBTQ folks on gender change. If I register a domain howtogetanabortionglobally.com, you may well understand somebody might be interested in finding out who is running that domain.

There's a carriage and content issue there, and ICANN is not engaged in finding out what you're using the data for, so therefore, we don't currently ask people whether it is sensitive to release their contact data in the context of a request from, let's say, a foreign government who doesn't believe in abortion or sex change or whatever the thing is. So that's a problem. It's a fixable problem by allowing people to say, "Do not release my data, whether I'm an individual or an organization, because it is sensitive under the European charter and protected," but we haven't dealt with that yet.

So I just wanted to sort of flesh out that aspect of sensitivity, and if you could just answer that question about the DPIA, that would be great. Thank you.

STEVE CROCKER: Let's see. Let me give the most embarrassing answer I can. We've not talked about or looked at DPIA directly, although beginning to engage in trying to understand what the legal issues are. Trying to build a somewhat neutral framework for expressing what the results of the answer would be if we looked at the DPIA and other things. And with respect to how to set the sensitivity levels, that is where people such as

yourself who are engaged in the policy discussions, what we're trying to do is provide an instrument for recording and comparing and analyzing what the results of such settings would be.

JANIS KARKLINS: Okay. Thank you. Last question or comment from James, and then we continue with our agenda. James, please.

JAMES BLADEL: Thanks, Janis, and I'm mindful of the time, so I'll try to be as brief as possible. Thanks, Steve, for this presentation. Just a question for you, and probably for Janis as well, we had this very intriguing model or architecture or approach. We had the Technical Study Group, and I think a lot of folks noted on the list that there was an announcement from PricewaterhouseCoopers of their idea. I know that I've personally been approached by at least a couple, two, three folks with their own models. Not all of these are completely incompatible with each other. And so my question is, to Janis, to Steve as a leader and a champion in this area and as to the rest of the group is, how can we best kind of synthesize all of these parallel tracks and all of these proposals and synchronize them with the work that we're doing on the policy questions to best arrive at something meaningful and useful, recognizing that we really have a very limited window to get to an initial report?

Again, I'm not really throwing sand on any particular the merits of any particular idea. I'm just trying to kind of formalize how we are going to corral all of these ideas and maybe pick best of breed and then move

forward into supporting the policy work. And I don't expect you to have an answer on that today, but I just want to put that front of mind for Janis and Steve in particular is that there's a lot going on. We have a very limited amount of time and bandwidth is very tight, especially the members of this group, and we really just need to find the most efficient way to leverage all of these really great ideas without slamming the door on anyone but also without getting sidetracked where we're just kind of spinning our wheels.

STEVE CROCKER: Sure. I was a member of the TSG, and as everyone understands, that was an ICANN-sponsored effort to do an RDAP-based architecture for nonpublic data for gTLD, for G information. We shared what we were doing, asked the natural sort of system architecture questions, could the TSG architecture support the kinds of policies that we were trying to represent? And the complementary question is the kind of policies that they expected might be asked of them, could we express them within our framework? And the answers were positive in both directions. So there was good mutual understanding. But they're completely separate otherwise. But good technical exchange there on PricewaterhouseCoopers, and I guess a similar in in respects effort by Mike Palage and Frank [Kona.] We've shared what we're doing with them and vice versa. That is complementary, in my view, and the piece ideally will fit together, although with the revision that's underway, probably have to have those discussions yet again. That's what's happening among the players that [inaudible] talked to PricewaterhouseCoopers.

With respect to from your point of view. How do you integrate all that? What do you pay attention to? Janis, that's your question.

JANIS KARKLINS: Yeah. Thank you, Steve, and answer to James' question is I proposed to invite Steve simply to stimulate our own thinking, and I hope that Steve's presentation now helped individually each of the team members to clarify their own vision of the task that we have to do, and hopefully, that will help us in our future considerations. So conscious of time, so Steve, thank you very much for joining us, and we will proceed with next agenda item, Any Other Business.

STEVE CROCKER: Thank you, Janis. Thank you, everybody. And I greatly appreciate your interest and your questions. My door is open if you want to continue to interact either as a group or individually, and I'll now break off.

JANIS KARKLINS: Thank you, Steve. So I will skip first topic, but I would like to ask members of the team to raise your hands – and Alex, please take it down for the moment – whether we should have next meeting on 20th of June or we skip that meeting of the team. So those who are in favor of or who are able to join team meeting of 20 June, would you be able to raise your hand now? So I think there is a reasonable amount of members who can join. So then we will have our next meeting on 20 of June at 2:00 PM UTC.

Then we have also sent around initial draft agenda for Marrakech meeting. We do not have time to talk about that now, but please, if you have any comments, please let us know, and we will try to factor them in our planning. And I see – so please put your hands down if you do not want to speak now. The last is to wrap up the meeting, and if may ask Caitlin to recapitulate all action points and all decisions we made during the call.

CAITLIN TUBERGEN: Thank you, Janis. The first action item I captured is for Thomas Rickert to provide a write-up of an IP infringement scenario to be discussed with the team at a future meeting. And Thomas is welcome to coordinate with support staff as necessary.

Second, the EPDP team to please review the list of purposes and third-party legitimate interests, and provide any additions, edits and comments by Tuesday, 18th of June, and also, EPDP team to please review the law enforcement example and be prepared to discuss this at the next meeting, which is confirmed for Tuesday, June 20th. Thank you, Janis. Back over to you.

JANIS KARKLINS: Yeah. Thank you very much. Is there anyone else wishing to take the floor at this stage? I see none. No, there is Hadia. Please, Hadia.

HADIA ELMINIAWI: Sorry, that's a mistake, because I was trying to raise my hand and it wasn't working.

JANIS KARKLINS: Okay. Thank you, Hadia. So that brings us to the end of today's meeting. So thank you very much for active participation, and so we will meet on 20 of June. In the meantime, please try to submit your comments on the list of purposes of third parties, and Thomas, please work on your homework that we can maybe look at it next time. Thank you very much, and this meeting's now adjourned.

[END OF TRANSCRIPTION]