MARRAKECH – GNSO-EPDP Phase 2 Meeting (2 of 2)
Thursday, June 27, 2019 – 08:30 to 15:00 WET
ICANN65 | Marrakech, Morocco

UNIDENTIFIED MALE: It is Thursday, June 27th, 2019 at ICANN 65 in Marrakech. This is the GNSO EPDP Phase 2 meeting, 2 of 2 at 8:30 in Hall Tichka.

JANIS KARKLINS: Good morning, ladies and gentlemen. Let us start our meeting today. I will assume moderation of today's conversation.

So I would like to start, as I was told that I have to start with the role call vote. No, with the role call presentation and if I may ask colleagues to introduce themselves starting from that side of the table please.

MATT SERLIN: Thanks, Janis. Yeah, Matt Serlin, Registrar Stakeholder Group.

OWEN SMIGELSKI: Owen Smigelski, Alternate Registrar Stakeholder Group subbing in today.

KRISTINA ROSETTE: Kristina Rosette, Registry Stakeholder Group.

MARC ANDERSON: Marc Anderson, Registry Stakeholder Group.

ALAN WOODS: Alan Woods, Registry Stakeholder Group.

DAVID CAKE: David Cake, NCSG.

MILTON MUELLER: Milton Mueller, NCSG.

AYDEN FÉRDELINE: Good morning. Ayden Férdeline, NCSG.

AMY BIVINS: Amy Bivins, ICANN Org.

DANIEL HALLORAN: Daniel Halloran, ICANN Org.

TRANG NGUYEN: Trang Nguyen, ICANN Org.

CAITLIN TUBERGEN: Caitlin Tubergen, ICANN Org.

MARIKA KONINGS: Marika Konings, ICANN Org support staff for the EPDP Team.

BERRY COBB: Berry Cobb, GNSO consultant.

JANIS KARKLINS: Janis Karklins, Chair of EPDP Team.

RAFIK DAMMAK: Rafik Dammak, GNSO Council Liaison.

LEON SANCHEZ: Leon Sanchez, Board Liaison.

CHRIS DISSPAIN: Chris Disspain, Board Liaison.

BEN BUTLER: Ben Butler, SSAC.

TARA WHALEN: Tara Whalen, SSAC alternate.

ALEX DEACON: Alex Deacon, IPC.

BRIAN KING: Brian King, IPC.

MARK SVANCAREK: Mark Svancarek, Business Constituency.

MARGIE MILAM: Margie Milam, Business Constituency.

ALAN GREENBERG: Alan Greenberg, ALAC, and to my right, almost soon Hadia Elminiawi.

GEORGIOS TSELENTIS: Good morning, everybody. Georgios Tselentis for the Governmental Advisory Committee.

CHRIS LEWIS-EVANS: Good morning. Chris Lewis-Evans with GAC.

ASHLEY HEINEMAN: Ashley Heineman with the GAC.

JANIS KARKLINS: So thank you very much. I would now like to ask whether agenda as suggested by Secretariat and distributed yesterday afternoon would be the one we would like to follow during today's conversation. Any objections? I see none. We will follow that agenda.

On the methods, I would suggest that we use the same method that we used during Tuesday's meeting. It is to say those who would like to intervene, please raise your hand in Zoom room. That would allow me to follow and provide opportunity to speak in the order that was requested from one side.

From the other side, I must admit that my eyesight is not any longer when I was 18, so as a result, I see all of you but a little bit blurry and I do not have red glasses to see very distinctively.

And also, thank you very much for those who came to me to introduce yourselves because until now, I knew many of you through photographs that staff provided to me. And it will take some time for me, to familiarize and become a fully-fledged member of the team. So therefore, please bear with me if I do not recognize some of you immediately.

Then also, for the sake of transparency, I would like to inform the team that yesterday I had a number of private meetings with the

IPC folks and with SSAC. They approached me, asked me to come to their respective places and I did that. We had a conversation about the process, expectations, a possible way forward, timeline, basically the things we normally would discuss in such a setting.

Next, I would like to maybe ask now Rafik very briefly, walk us through the results of Tuesday's meeting and see whether we share that assessment that will be provided now by Rafik. Rafik, please.

RAFIK DAMMAK: Thanks, Janis. So on Tuesday, following our agenda, we tried to go through the template using [inaudible] that was proposed by Thomas, and based on the discussion at that time, we decided to begin with the [inaudible] entry. And so we tried to get input and suggestion, including even maybe changing the format there.

So for that part, we agreed as an action item that the staff will review and incorporate the input for that use case and distributed to the team, and I think that was already done with a clean and redline version, and you will see that the document also changed a lot in terms of the format.

And also, we asked the team members to think about other use cases. On the other hand, we had during our lunch session, working plan session, two presentations from groups that they're working on some implementation and in the way maybe to get some idea about what can, I'd say, about maybe kind of visibility approach here.

So other than that, so prepare it for this today meeting and I think that's what we will continue to do, I mean, in terms of continuing our deliberation that started on Tuesday.

JANIS KARKLINS: So thank you very much, Rafik. Are there any comments at this stage? So I see none. Then let us proceed to the next sub-item objective for the day.

So I think that the agenda is self-explanatory and we would engage with ICANN Org Strawberry Team to get information, what is happening on that front in the context of ICANN Org with the European Data protection authorities and European commission. There will be opportunity to ask questions of all kinds in relation to that engagement. As a result, we will draw conclusions and whether any action from our side is needed at this stage.

So then we will move to examination of the case that Thomas kindly put forward and that will be a second reading, and hopefully, the last reading of the case. We will take as much time as needed. The time indicated in the agenda, of course, is tentative and we will not follow exactly as-is, but we will take as much time as we need or if we examine agenda item earlier, we would go to the next one.

So, and after that, we will start examination of the next case in public safety that was prepared by GAC representatives. We will listen to the presentation and hopefully, we will be able to make a first reading of that case.

And at the end of the day, we will go and try to agree on the list of cases that we would examine, as well as we will discuss the way how we could go through all the cases in the most efficient, and what would be our next steps until our next face-to-face meeting in Los Angeles in mid-September.

So these would be broadly things that we would try to achieve today, and I now open the floor if there are any comments or objections to that proposal. So I see none, so then we can proceed to the next agenda item, and that is engagement with ICANN Org.

Elena, would you join me please? So thank you very much, Elena, for joining us. And so at the beginning, we would listen to the presentation of Elena on the state of play and whatever news Elena would like to share with us. After that, we will open floor for comments, questions. With that, Elena, the floor is yours.

ELENA PLEXIDA: Thanks so much, Janis. Good morning everyone. Hello. Nice to meet you. I do not know every one of you. Thank you for inviting us here to have this discussion with you today. We've put together some slides to help surface the topics and supportive discussion, and of course, then open to any other points that you want to bring in.

Can we move to the next slide, please? And next slide?

Okay, so we'd like to present ourselves to you, first and foremost, and then discuss about the task that was given to us by our CEO and the Board, and have a discussion about the Unified Access Model based on the DSG Technical model. What is the basic assumption behind it? And essentially, what it is that we are going to test with the DPAs in Europe. Chat a little bit about the process environment and the engagements to date with the European Data Protection Boards.

And as I said, then open up the discussion to these points or any other point that you would like to [inaudible]. Next slide, please.

Right. So the ICANN Org team, which also goes by the name "Strawberries", and here, I need to make a disclaimer. We are not responsible for our name. We didn't pick it, but here we are now.

The ICANN Org team consists of the following colleagues. It's Daniel Halloran from Legal, Amy Bivins, also Legal, John Crain, Octo, Francisco Arias from GDD Technical Services. [Eliza] [Gobian], MSSI, Diana Middleton, MSSI, and myself, Elena Plexida.

And I'm part of the Government Engagement Team. I'm based in the ICANN office in Brussels and as one can probably tell by my location and the team I work for, my main focus is, among other tasks, the European institutions. And in fact, I come, myself, from the European institutions

Now in our team, Francisco and Jonah, the technical experts, they were also supporting the work of the TSG Group. So did [Eliza] and Diana. Dan and Amy obviously bring the legal side in our team and Dan, moreover, is, of course, the liaison to the EPDP team. Next slide, please.

What is the task that has been given to us by our CEO? It is pretty straight-forward. It is to bring forward to the [place], the UAM based on the TSG model with a view to test its basic assumption, and therefore, test its visibility under the GDPR. The aim of this whole exercise is to bring back input, to bring back a response to the EPDP team, to you, available for your consideration as you work to develop policy for standardized taxes for gTLD registration data. Next slide, please.

Now with respect to the need for registration data access or a disclosure model, and more particularly, the approach of a unified model, the ICANN Board has consistently recognized that enabling access to GDPR registration data is an important mandate for ICANN. This has been reiterated by many stakeholders, including the GAC. The contracted parties have stated that a centralized access portal might result in a more predictable and uniform experience for those with [inaudible] and proportionate interest in user registration data. Next slide, please.

The European Commission has encouraged us to develop a unified access model and they call this work vital and urgent. The new member states have adopted the lines to take in the context of the EU Council, and there, among other considerations, they have supported the development of a unified access model that applies to all registries and registrars, and provides a stable, predictable and workable method.

If this [inaudible] to take, which is an, official document of the EU, they also describe the [inaudible] situation that exists today as problematic, and of course, continue saying we have to find a solution as soon as possible. And just this week, we received a letter from G7, the G7 High Tech Crimes Sub-group calling ICANN to quickly implement a unified solution and they conclude by saying that this is a necessity for public safety. Next slide, please.

Now if we're talking about a unified solution, and I put emphasis on the word "unified" because solutions could be, obviously, many, we believe that the only way to have a unified solution for access to nonpublic registration data is by sifting away the responsibility from the processing activity of disclosure, and therefore, the risk associated with the processing activity of disclosure from the contracted parties. Again, I put the emphasis on unified, and when I say unified, I mean in terms of achieving the highest possible level of consistency and predictability with respect to someone who has a request, knows where to address the request, and with respect to predictability of getting an answer, even if this answer is "I'm sorry, you are not entitled to have access to this data," and also for the contracted parties that are involved in a model.

Now, Francisco, my colleague over here, will now briefly explain how a UAM based on the TSG model could work.

FRANCISCO ARIAS: Thank you, Elena. I work for ICANN Org on the technical side and I was part of the, excuse me, TSG group. And so, as Elena said, the idea is to have Org to show a unified access model based on the TSG model, and what you see here in the slide is a high level diagram of the TSG model. The TSG model provides for options or [inaudible] options if you life on deciding, particularly, who will play the roles and that's something that is not a technical issue.

And so there are three main roles that are played in the model, the TSG model. The first one is that ICANN are the [inaudible] service or the central gateway that is also called the TSG model, so one that is in the center. That is the service to which all the [inaudible] for nonpublic registration data will need to pass. So that role will be played by ICANN in such a model.

There is also two other key roles that are shown in the slide. The one two below the central gateway called the NT providers, that's the role, that's the providers that will take care of authenticating their requesters. So for example, they will take care of accrediting that someone is a law enforcement agent from a certain agency or a security researcher from an appropriate organization, and so on and so forth.

And all of this is, of course, depending on whatever the policy says. We're not assuming that someone will get access. These are just merely examples of what could be. It all depends on what the policy says.

The important [bid] is that the NT providers are in charge of accrediting, that's, let's say, offline. By offline, I mean before any [party] is submitted and they are also in charge of authenticating our requests, or at the time, they are making a [inaudible].

The tier role that is key in this model is the authorization service, the one at the bottom. That also can be played by one or more organizations. It depends on decisions that are not technical. This party or parties are in charge of applying the policy, the TSG model, assuming there will be a policy defining what are he conditions, who will access to what fields under what circumstances, etc. And so this authorization service, these authorization parties will be the ones in charge of applying the policy and providing, at the time a query is made, providing the response to the central gateway saying this party is authorized to access this data or no, they are not.

And supposing there is a positive response to that question, then the central gateway, another key point here is the central gateway will ask the relevant contracted party's servers for the registration data. It is envisioned that it will be for the registration data. This is in line with what Elena mentioned, that the idea is to leave the contracted parties with, if you like, isolated as much as possible from the query that is being made and from who is making the query so they will not know who is asking. Of course they need to know what is being asked in order to provide the data.

But if they were [inaudible] to finding who has access to what, they would not see that. They would simply return. They will be expected to return the full data and then the central gateway will be the one applying the profile and filtering and providing to the requester only the data they are authorized to send. So this is a high level review of the model. Thank you. Back to you, Elena.

ELENA PLEXIDA: Thank you very much, Francisco. Okay, now, as you can see by what Francisco explained, this model is, which is a technical model essentially, but it's based on a very simple notion that the contracted parties who are holding the data would not be part of the adjustment, would not be part of the decision making when it comes to who has access to data and which fields, etc. etc.

It is a very simple idea, and this, a very simple assumption. The assumption is the following, that if you are not part of the judgment, if you are not part of the decision, you might hopefully not be liable for this decision, for this judgment. And it is this, as I said, is just an assumption. It's just a theory. It is an assumption that we make.

The task of our group is to test this assumption with the DPAs, is to ask the question "Does it work?" or "Does it not work?"

If this theory tends to be wrong, then [inaudible] that the unified access model is not possible under the law. So this is the question that we're going to the DPAs with. We would like to have, we'll try to have a clear answer to that so as to be able to bring it back to you for your considerations, and I mentioned before I need to make an important clarification. It's already obvious from what we're discussing, but just to highlight that when we're talking about no liability, we're talking about only the processing activity of disclosure. It is obvious that the rest remains with the contracted parties as they should remain.

Now, and no – and I highlight that – and no is also a good answer. We consider that a no is also a good answer from the [inaudible]. We know that that means that we know what's possible and what is not.

We will continue to brief you as we go along with this exercise and publish our relevant material, and obviously, we're open to your suggestions with respect to engagement.

Let me briefly mention where we are right now as a team. You know better than us because you have been involved in this exercise of considering questions or input to the European Data Protection Board. You know very well that the input you give to the Board has to be as relevant as possible so as to actually have a meaningful output. The better the input is, the more precise, the more specific the answer will be, and that's what our team is doing now. We are [inaudible] how to give this input to the European Data Protection Board. Obviously, you cannot just give them the TSG report as an example and tell them, "What do you think?" That's not answer. That's not the question. They're just going to quote back to you articles from the GDPR. So that's meaningless.

So therefore, we're working on that. Will it be a paper? Will it be questions? Will it be both? That we'll elaborate on the basic assumption we just made, introduce the question, "Does it work?" and also state that any policy considerations with respect to who gets access to data, what kind of data under what [circuit] is not the part of this exercise and this completely belongs to the EPDP team that is responsible for developing the policy. Next slide, please.

Yes, I already covered that. Next slide.

Okay, and now I would like to refer a little bit to the [inaudible] environment, not all of it, obviously. The one that is relevant for us, for ICANN and for our discussion with respect to the registration data and GDPR.

And obviously, [inaudible] we have the European Commission with us in the EPDP [inaudible] way is the European Commission. The European Commission is a big animal. Let me put it that way. It consists of many, many [inaudible] and agencies. The one that are relevant for us are the following. It's Digital Connect, DigiJust, Digihome, legal service, and secretarial general. Digi Connect is the [DG] that is in charge when it comes to relations with ICANN, so Digi Connect is in the [inaudible]. Yes, Georgios is over there. It is the DG that sits on behalf of the European Commission in the GAC and brings all the rest together in this exercise.

DigiJust is the one that drafted the law. You know that very well. Digihome is [inaudible] first and we also have legal service and Sec Gen. Sec Gen, let's say, is the [inaudible], the one that organized the commission [inaudible] all together. So you see that even within the commission, the balance between the rights to access and the right to privacy is being considered and Georgios is bringing all this together.

The Commission is the legislative initiative. That's something to remember. IT means that they are the ones that drafted the law. Then they give it to the council of the European Parliament and it becomes legislation, but they are the ones that drafted the law. Next slide, please.

Now the GDPR, though, is interpreted and enforced by the European Data Protection Board. They are responsible for anything. They consist of all national DPAs, the European Data Protection Advisory and the European Commission. The European Commission sits, DigiJust sits in the European Data Protection Board, but with no voting rights.

No the Data Protection Board organizes its work through expert sub-groups. The one that is looking at the registration data issue, the ICANN issue is the technology sub-group. So whenever there has been a physical meeting between ICANN and the DPAs, it has been with the technology sub-group. The technology sub-group then raises it up to the Board, to the plenary, and we have been receiving, the letters we have been receiving [inaudible]. I'm sorry for that.

All right. Why am I mentioning all that? With respect to this exercise of testing the assumption we mentioned before, we would like to have an answer as soon as possible, but not everything is at our hands. The European Data Protection Board comes together as a plenary once a month, and the next plenary is already taking place on the 9th and the 10th of July which means that we do not have time. We also have to factor in that you first have to go to the technology sub-group and then it goes back to the plenary. August is a dead month for Brussels, so there is no plenary meeting, which means that what we can hope for, we'll aim for, is the September plenary meeting of the EPDP.

That's just the timeline. It is to be confirmed, of course, because there are variables but I'm just giving you a speculation. Next slide, please. Thank you. Okay, this is a slide and the next one, as well, with containing engagement activities that have taken place so far with the European Data Protection Board. And next slide, if you may.

Out of this, you should keep that the last time we physically met with the technology sub-group was on the 23rd of April last year. We haven't met them since the summer. All the relevant activities, actually these slides contain the most relevant ones. All the others are published in the data protection correspondence and [inaudible] of our side. Next slide, please.

And finally, this is the last slide and I will close with that. It is about the purpose of engagement. I'd like to highlight with you that, of course, the main purpose when engaging with the Data Protection Board and the authorities in Europe is to obtain guidance, to lead our work here. But I also wanted to highlight that we should not lose sight of the fact that it is important to demonstrate the ICANN community efforts to comply and this is part of the engagement. It is in the spirit of GDPR to demonstrate, to show that you are meaningfully doing efforts to comply and also, there is understanding. Promote understanding about what is happening and how difficult it is for us.

As I mentioned at the beginning, I come from the European [Institution] myself and when the whole discussion started, I was sitting at the other end of the table, if I may put it that way. And I can tell you that the level of understanding in the Brussels bubble, and I include myself in that, was the following. There is one database, contracted parties [inaudible] contracted parties. ICANN has a database. You can just change it and fix it like every other platform will fix it. We're far away from that now, of course. I just want to highlight that engagement is not only about obtaining guidance or specific questions. It is about raising awareness in Brussels about all the efforts that the ICANN community is putting together. And I will stop with that and hand back to [inaudible].

JANIS KARKLINS: Yeah, thank you very much, Elena. Now floor is open and as I suggested, please raise your hands in Zoom room and I will take this from there. I see that Milton is first asking for the floor. Milton, please go ahead.

MILTON MUELLER: Yes. Good morning, [inaudible]. I'm sorry that you've been put in this position. We really are kind of dealing with a distraction here from our work.

First, we were told that the technical study group was a purely technical exercise, that they were testing and developing technical solutions. Now you're telling us that you're taking this model that they've developed to data protection authorities and asking, "Can we test its basic assumptions and feasibility under the GDPR?"

In other words, you're telling us that there are policy assumptions built into the model that may or may not be consistent with GDPR because its acceptability under GDPR depends entirely on the policy assumptions and on the policies that guide it. It has nothing to do with the technical matters. So you have immediately confirmed all of the fears that we had when the TSG was created was that it was a preemptive move that would undermine or otherwise substitute for the work of this group.

Now let me just say that, again, whatever conversations you have with the DPAs will depend entirely on the policy assumptions that we create and developing those policies is our job, not yours. I repeat it is not ICANN Org's job or the TSG's job to be developing policies. It is our job and it's extremely destructive of the ICANN regime for that role to be preempted or subverted by the Board.

Now I hear again and again this line that your work is supposed to feed into or contribute to ours. I don't see how it does and I don't think I'm being cantankerous. There is not a single sentence in your presentation that shows any awareness of the recommendations that we developed in Phase 1, not a single point. You even use a language, a label, that we have rejected. We are not talking about a UAM. We are talking about an SSAD. Could you at least adopt the language that we're talking about so that there is consistency between our efforts?

So I guess the question is tell me how this works and how your independent and parallel interactions with DPAs contributes to our work. For example, we've had a very interesting and constructive debate about the degree to which trademark owners can make certain numbers of requests and how those requests will be handled. How does this model of yours help us resolve those policy questions?

JANIS KARKLINS: Thank you. I do not see any hands up in the Zoom room.

LEON SANCHEZ: Thank you very much, Janis. Let me try to do a second go on the explanation of why this is being doing.

The TSG, this diagram that has been represented, is just a technical model. We have to look at this effort in a realistic way and try to understand that there are at least two parts to it, one that is technical, which is the diagram that we just see and another one that is legal, which is the work that the EPDP is undergoing. So that is how the two pieces of the puzzle, Milton, feed in together to try to have SSAD. Right?

So having this process, this technical consultation, about whether a technical model like the one presented could be feasible under GDPR does not substitute in any way, from my perspective, the very important work that we are all doing here in this EPDP.

So all that the TSG has been doing is just to create a technical alternative, just another option to consider by the EPDP. So we are now in a fork in which the organization will submit this to the data protection authorities to ask whether this is a feasible model or not. If it's not feasible, then that's it. That's as far as the TSG model got, right? If the European Data Protection Board says, "Guys, this is just not workable. This is not feasible under GDPR," then that is as far as this goes.

Then if we have a positive reply by them and they say, "This actually could work," then this technical model would feed into the EPDP process to inform us all that there is a technical part that is actually compatible with GDPR as designed by the TSG. On top of that, you need to match the legal situations, right, the policy job that Milton was referring to. So once you match the policy that we are doing in this EPDP to the technical design that the TSG has put, then you have the two pieces of the puzzle together and you could actually try to implement the solution. Right?

So as I said again, this is not a substitute of the EPDP work because the EPDP work is the policy to which the technical model will actually match to be implemented and not the other way around.

JANIS KARKLINS: So thank you [inaudible].

OWEN SMIGELSKI: Owen Smigelski, Registrar Stakeholder Group. So I appreciate the work and the effort on this, I would like to echo some of Milton's comments as well too. If when this working group comes up with some sort of different model, the SSAD model, would ICANN Org go through these same activities to actually present what the GNSO Council [decides]. I think it's a bit premature at this point to keep going through this because there are a lot of assumptions baked into this. It is, yes, purely technical but there is a number of policy assumptions that are in that as well too, and that may be a little premature to [inaudible] these efforts. So that's the first point.

The second point is all these communications that ICANN Org is having with the DPAs, will ICANN be sharing that with the working group? Because there seems to be a number of communications both ways. I know some letters are published online, but that does not appear to be all the communications that are ongoing and whether they are favorable or unfavorable results from the

DPAs, it would be good to have that shared with the working group so that can guide our efforts.

JANIS KARKLINS: So thank you. Georgios is next followed by Megan, Margie.

GEORGIOS TSELENTIS: Yes. Good morning. Good morning. Thanks, Elena, for the presentation. I will mention first something about the assumption and how it's formulated. I think when we go to interact with the data protection authorities, it's good not to say how we are going to get rid of responsibility of some parties, but it's better to say who takes responsibility and that's to be very clear. So the DPA wants to see. Their mindset is data protection and they want to see a clear formulation of whatever model is going to present or whatever procedure. It has to be very clear how data owners' rights are protected. So I think it's a question of language and how we present things, but I think it's very crucial not to start with the assumptions that maybe are of interest for some parts of the community, but go and test the basic question with this in mind.

Now going to what Milton said and what are the concerns whenever we get presented by any parts of the constituency of models, I think we got presentations, I think two models now we had also Steve Crocker presenting, so there are several models there. I think the value of those models is great because we visualize parts of the implementation, so we get the frame of what is a possible implementation, and then on top of that, we can test the legal implications of doing so. There are so many things that we have in front of us – I can mention data transfers among jurisdiction to name a few – that are not so easy to deal with if we keep the abstract layer of just developing policy.

So I welcome very much any part of the community that wants to put on the table a model, and when I saw the TSG model, I thought it was a very, very useful exercise because the people who developed that were knowledgeable about the functioning of the RDAP. And so I think this is extremely helpful that without considering that this is framing us in order to decide policy-wise what is allowable and what is not, it gives us a visualization on many of the questions that we are dealing with in our template.

We have the template which was presented by Thomas. We are going to present to you a template later on from the law enforcement point of view. So it's very, very useful, I think, and I believe this is the way we should go on if we want to achieve any results. I'm not talking here about, I don't know, for two more years about the possible policy that we could develop. It's very useful to try to map the policy, and here again, I agree with Milton in this that it's not the policy that has to be guided by the technical models, but it helps us very much to develop our line of thought. Thank you.

JANIS KARKLINS: Thank you, Georgios. Next is Margie, followed by Mark SV.

MARGIE MILAM: I just want to say thank you to ICANN staff, the strawberry team, for putting in this kind of thought. I think it's exactly what we need. As we were working in Phase 1, a lot of the decisions we were focusing on and we will be in to Phase 2, is how to minimize liability and I think the questions that you're posing, essentially, answer some of those questions.

Now we'll take those answers and decide whether it fits into our policy, but at least it addresses where the policy can go. And so I think that this is a great idea. I think that it'll inform our work and I think it's timely.

JANIS KARKLINS: Thank you, Margie. Mark SV. followed by Brian King.

MARK SVANCAREK: Yeah, I have to agree with Milton on part of his intervention that the model that is shown here doesn't have anything to do with the policy we're developing, so that is true, and therefore, we need not consider that model in any of our deliberations unless we choose to do so.

But I also have to agree with something that Margie said. There has been a repeated assertion that if a third party makes the decision, whether that's via accreditation or ICANN or something else, that this would somehow reduce the liability of a contracted party, and as Alan has pointed out many times, there is actually no evidence that that is true.

So it's good to have a process whereby we can get at least some certainty whether or not that assertion could possibly be true and I recognize that a DPA can't talk in generalities, that they must be presented with a specific scenario in order to even consider evaluating such a thing. So in spite of the fact that this model has nothing to do with the work we're doing here, it does provide a form of specificity which can be used to test that assertion and so that nugget, that little piece of is the involvement of a third party through accreditation or other going to have any benefit to a contracted party? I think it's valuable insofar as it helps to answer that question. Other than that, it's safe to disregard this model I think. Thank you.

JANIS KARKLINS: So thank you. Colleagues, I would like to say that the time is running and I have a long list of speakers. So we have Brian, Stephanie, Hadia, Alan, Alan Greenberg, [inaudible], Marc Anderson. And with your permission, I would draw the line here with these interventions. So please now, next is Brian followed by Stephanie.

BRIAN KING: Thanks, Janis. I'll be brief. I want to say thank you to the strawberries and to ICANN Org for helping us with this input. We've been wondering, I think, as a group, I think, what conversations are happening with the DPAs and the European Commission and how those are happening, so the insight is wonderful and we appreciate that.

The IPC understands the technical study group shows a technical model is possible and that's what we take from the TSG, and we encourage and appreciate that assistance from ICANN Org. We understand that this effort shows that this may be legally sound and to that extent, we encourage ICANN Org to undertake this and we appreciate that assistance with that, and we fully believe that the EPDP team can then use those inputs or not as we go through our policy development, but we really value this effort and thank ICANN Org and the strawberry team, which I'm still struggling with, to continue that work. So thank you.

JANIS KARKLINS: So thank you, Brian. Stephanie is next followed by Hadia. Stephanie is joining us remotely. So Stephanie? You should unmute yourself. While Stephanie is unmuting herself, I would call on Hadia.

HADIA ELMINIAWI: So if we can scroll back to the diagram, the model itself. So looking at the model, I actually see no policy assumptions here. What I only see is assumptions in relation to how our policy is going to be implemented, and the main reason we have such an assumption for an SSAD or unified access model – well, names don't really matter – is to reduce the liability on the contracted parties.

But again, looking at the model, we look at the box for the registration data. That's our work. That's what we determine, right? What is the data that's in this box? The authorization services, what are the basis in which authorization is going to be given. That's, again, our work.

So all of the boxes in there, looking at them, it's actually what we are doing. It's our policy. What's there, it's only how this policy is going to be implemented and that's the only assumption. So it's an implementation assumption for the purpose of reducing the liability of the contracted parties, and if it doesn't work, then we will need to see another how, and that's fine as well.

But as far as we are being concerned, all of the boxes in there is actually our work. Thank you.

JANIS KARKLINS: So thank you, Hadia. Now we will try with Stephanie.

STEPHANIE PERRIN: Hello. Can you hear me?

JANIS KARKLINS: Yes, Stephanie. We do hear you. Please go ahead.

STEPHANIE PERRIN: Wonderful. Thank you very much and I apologize for being remote. I'll be there shortly.

I would just like to remind this group that the NCSG held a privacy meeting to which they invited representatives of the European Data Protection Authorities in 2014 when the EWG report was released. We got the technical study group people there. They are well-aware of the possibility of such a system and what it could do. The fundamental legal question here is can such a system remove liability from the contracted parties? And it does seem to me that this is what this lobbying effort is about.

Now unfortunately, the noncommercial stakeholder group was not included in the – I don't know whether it's the strawberry group I should be referring to or the technical study group – but we had no representatives and most of the other stakeholders in this room had representatives there.

And, of course, we are, therefore, not included in this lobbying group which I thank Elena for the brief description of how the European Commission works.

I don't think, while I have great sympathy for my colleagues in the contracted parties, with respect to liability, I don't think that the policy objectives of the noncommercial stakeholders group, which is, after all, a legitimate member of the GNSO, are aligned here. We do not wish to remove liability to some intermediate actor because partly, some of us are active in the civil society arena and we don't wish to see this replicated in other fora as well. ICANN is not the only creature in the universe, so this is a very big policy issue that we are talking about here and it should be open to all stakeholders. So we would like to either come along on any lobbying party that goes to Brussels to discuss this with the European Data Protection Board either in their meeting or outside their meeting, which is the normal method, or we would like advice from ICANN staff in a non-partisan way as to how we can go to Brussels ourselves and lobby. Thank you.

JANIS KARKLINS: So thank you, Stephanie. Maybe it would be now time to remind ourselves that the offer of CEO and President of ICANN is still standing, that we can provide whatever policy questions we deem to be appropriate being asked to European Data Protection Authorities and channel through the strawberry team to get those answers.

So I understand that on Tuesday, one question came out that would merit being transferred and asked to European Data Protection Authorities, and that is about the liability of requesters, whether we could factor that in, in our policy discussion, that requesters are liable also for putting their requests based on sound legal basis and purpose. And if we would verify that this assumption is correct, I think that that would help us also move forward in our policy discussions. So with these words, I now turn to Alan Greenberg followed by Amr.

ALAN GREENBERG: Thank you very much, and I guess I'm speaking on behalf of a not legitimate part of the GNSO, but I thought a legitimate part of this EPDP.

I can't speak to whether a group here wants to see liabilities moved, changed or not. I don't think that's part of the formal policy we're looking at. I, and I'm not unique around this table, but I've got a very long history in comparing complex system design and implementation, and the only way to do that kind of thing is to work in parallel. Yes, occasionally, you will do something and then have to loop back and do it again in a different way because of what's going on in the other parallel streams, or more than occasionally. You're almost guaranteed to. But if you don't do things in parallel, if you serialize every part of the effort, the implementation time becomes unreasonable and sometimes totally unfeasible. So I strongly support what we're doing and I wish you continued luck, and we will do anything we can to try to support this and try to make sure it works. I don't see any other way to get around this but to work in parallel.

Whether our final system is completely manual or completely automated, it's a complex system and it's going to be difficult to implement and we need to look at all aspects as we go forward. Thank you.

JANIS KARKLINS: So thank you, Alan. Next is Marc Anderson. Sorry. Next is Amr followed by Marc Anderson.

AMR ELSADR: Thanks, Janis. Alan, appreciated everything you said. But again, going back to Milton's earlier comment and some of the responses by Leon and Chris, the ICANN bylaws say that the GNSO is responsible for developing gTLD policy. There are operating procedures and GNSO working group guidelines on how that is done.

Part of those is that members – they don't have to be affiliated with the GNSO – GNSO policy development is open to other SOs and ACs as well, but members have to engage. They fill out statements of interest. We know who they are and the working group itself will work to develop policy recommendations, and there are existing rules and guidelines on how to seek input from external parties.

Whatever the intentions, whether they're good or bad, whether they're meant to be constructive or not, is not the point. The point is that we have certain expectations on how we're supposed to be doing our work. We develop work plans accordingly. For ICANN Org to make assumptions on their own and undercut our work is destructive to what we are doing. It's problematic. It also, to a large degree, might influence the agenda of what we are doing. We don't want that. We never asked you for help.

When the CEO engages with this team and says if there are questions, we want to ask the DPAs, we would like your input, what do you think, that's fine. This is the sort of engagement we should have early on at the beginning of the process. But to come up with an initiative completely begun by ICANN Org and then to feed into our process, this is not helpful at all.

So I don't want to have the last word on this. Meaning this is what we have, we're coming up with it and you do with it whatever you want. It becomes extremely difficult to ignore. A lot of financial and human resources were put into this. We don't have much of a choice on what to do with it, not really.

Now that it's here, at best, we will be divided on what to do with it. Engagement on this should have begun at a much earlier phase. The working group never asked for it. The working group Chair never did. The chartering organization didn't. It was a purely ICANN Org initiative and it shouldn't have been done this way. Thanks.

JANIS KARKLINS: So thank you very much, Amr. Next is Marc Anderson and then we had earlier also, Thomas in line. Since he is remotely, he took off his hand. Now he's back in line. So Marc followed by Thomas.

MARC ANDERSON: Thank you, Janis. First, let me thank Elena for coming to us and telling us about the strawberry team and what you're doing. I appreciated that and I learned a bit from the presentation, so it was good getting that information and hearing from you.

And I think hopefully you've also heard from us and be able to take away some of our frustration, some of our challenges, some of the things that we're wrestling with trying to figure out how to go forward with this EPDP Phase 2 task we have.

But sort of absorbing all the comments and everything we've been talking about, I guess what I'm thinking is how do we move forward from here? What's the best way to move forward? So I'm wondering will you be a liaison? Will you be somebody that's going to work regularly with us? Will we be able to have regular interactions with you? What's the best way to move forward from here? I think we can retreat to our corners and choose not to work together or we can figure out what is the best way to work together towards getting to an EPDP outcome that everybody can live with.

So I guess I'd like to challenge all of us on the EPDP team to figure out how to work together with ICANN Org, how to work together on figuring out the best way to interact with the EC and DPAs and I'd like to hear from you what is the best way that we can work together in your view moving forward. Thank you.

JANIS KARKLINS: So thank you, Marc. Thomas is next.

THOMAS RICKERT: Thanks very much, Janis. And thanks very much, Elena, for your presentation.

I think that my primary concern is that if you look at the communication that ICANN had with the Article 29 group at the time and then the European Data Protection Board, you could sense a frustration with those buddies in communicating with ICANN because ICANN did not really offer solutions, but just asked questions. And I'm afraid that we might run into the same issue. I think we only have one shot at this, to ask the commission or the data protection board for their advice. It can be iteratively, but I think if we frustrate them with half-baked solutions, they might not be willing to engage further. And therefore, I think, yes, we should engage with them. This is part of our thinking all along. We need to get early thinking from the authorities to check whether we're on the right path with our thinking, with our policy development. But I think that at this stage, it's premature to confront them with primarily technical considerations.

The European Data Protection Board will look at this through a legal lens, not through a technical lens, and we have not sorted out basic questions. Göran made it very clear yesterday during the CSG meeting that his goal is to get clarity on the liability question, and I fully agree with Georgios that starting with that might not be the best idea. I do appreciate Göran's intentions to get clarity for the contracted parties in particular, that they will not run the risk of being sanctioned if they engage in whatever disclosure model we come up with.

But I think we should come up with concrete proposals, and that includes the question on how the contracted parties will work together with ICANN, who is going to be responsible for the disclosure and the accreditation, and also the safeguards involved.

And I think the combination of technical considerations and a rough technical setup will enable the European Data Protection Board and the commission to give preliminary answers. But ultimately, and I think this has been discussed in our group earlier on, I think there is no way that even the European Data Protection Board could, if it wanted to, write a blank check to ICANN that there will be no liability. I think the only legally viable solution is for us to describe a path towards a code of conduct, get a code of conduct approved, and then those who will play by the rules of the code of conduct will not run the risk of being sanctioned.

So in short, yes, we should engage. Thanks, Elena, for the work that you and your colleagues have put into this. But let's wait a little until we have more clarity on where this is going and then go to the authorities with robust and well thought-out proposals. Thank you.

JANIS KARKLINS: So thank you, Thomas. And the last speaker is Chris Disspain.

CHRIS DISSPAIN: Thank you, Janis. Good morning, everybody. I just want to make a couple of points.

First of all, just to be clear, this is not an Org initiative as such. This is the Board telling the CEO that one of its goals is to find out whether or not a model, an access model – and I'm not interested in debating what you call it for now, we all know what we mean – an access model is workable or not. And the only basis upon which we see that it would be workable is if there was a way. We might be wrong about this, but the only way we see it would be workable is if there was a way of removing the liability on the contracted parties. And in that case, it may be that such a model is workable.

Now without input from the DPAs, then the only possible outcome is to say that it isn't legal because you can't disprove the negative. So it may be that it isn't legal. It maybe that it is. But unless we ask the question, we're not going to know the answer.

So in an ideal world, you develop the policy and then see whether it's legal but that's not going to work from a timing perspective.

To be clear, we're not seeking to develop policy here. We are not saying there should be an access model. We're not saying if there is an access model, how the technology should work. This is merely an example of how it could and if I do remember correctly, this input from the technical group was welcomed by the members of the EPDP.

It's clear from the discussion in the room this morning that some people think that going out with this question – and it is a question – is good and some people think it's bad, so there's no surprise to that. The only other point I would like to make is that in respect to the disclosure of communications between ICANN and the DPAs, all of those disclosures, all of those communications – I'm sorry – have been disclosed and my understanding is – I may get the dates wrong here, but my understanding is that there hasn't been any communication between ICANN and the DPAs for quite some time, August, I think. I could be wrong about that. So to suggest that there are communications happening that haven't been disclosed is simply incorrect.

And the final thing I'd just like to ask you all is – and we would need to take this back – is I assume you would like Elena and the strawberry group to interface with you on a fairly regular basis and if that's the case then we will see if we can organize for that to happen so that this doesn't disappear into a black hole because even if we go ahead and ask this question, or when we go ahead and ask this question, it's not going to be answered within a week so you probably want to keep talking. Thank you.

JANIS KARKLINS: So thank you, Chris. So after this, [inaudible] if I may say, so you heard a lot of opinions of the team members. You also heard a number of questions. I understand that you will not be able to answer each of them, but you may want to cluster them and also provide some clarification and, of course, the big question is how to move forward with our interaction and communication. So Elena, floor is yours.

ELENA PLEXIDA: Thank you, Janis. Indeed, thank you for this input and I'm not sorry at all for myself, for being here with you today, Milton. I think it's very valuable for me as well to get all the input, be it frustration.

At the beginning, when I started speaking, I said that the EPDP Team is working to develop a standardized model, an SSAD as you call it, I didn't use the acronym. And what we are suggesting here is just one possibility, one possible standardized and I said that it could be several others, obviously. The idea that we're presenting to you, again, is very, very simple, is an idea that would have the contracted parties out of the judgment and the reason we're doing that is to check the question. Does that work?

I think that Marc put it better than me. You cannot talk in the abstract with the European Data Protection Authorities and that's also something that Thomas said. Thomas said that there was frustration because we did not offer solutions; we only asked questions. We cannot just ask a question. Is there a way that the contracted parties would be not liable. That's nothing. We will get back nothing. We will just get back a quote from the GDPR. If we present an idea, just an idea, even if it lacks all the policy considerations, then you have a chance to get an answer yes or not. And I repeat, a no is a good answer to our mind because then you know that this is not a possibility. It's not a possible option for you to consider. At any rate, that of course remains with the PDP to decide whether to adopt the policy later on that employs this technology or any other technology or in what way it will employ this technology.

With respect to what Georgios said about liability, not start with a question of liability, I understand – Georgios, correct me if I'm wrong – I think Georgios means do not ask the question. Georgios means that when you talk to the European Data Protection

Authorities that are responsible for privacy, you don't talk to them about liability. You're talking to them about who is having the responsibility of taking care of this processing activity in the best possible manner. I see Georgios nodding. Maybe I got it right.

And also, the European Commission has a committee to facilitate this interaction with the European Data Protection Board so as to be able to get this answer. And I suspect all later interactions.

Now another question I received was whether we are going to check any other model or any other questions. Of course. At any rate, what our CEO had said, any questions that you have or anything what you want checked with the DPA, we're more than happy to bring it forward [inaudible]. With respect to ongoing engagement, if you would like to continue the interaction with me, if you'd like me to be a liaison, if you would like me to play any other role, yes, we are more than willing to continue that. And I'm sure I missed many other questions. I'll stop here.

JANIS KARKLINS: So thank you, Elena. We note your willingness to interact with the team at any time. We would invite you to join us. So I also think we always need to keep in mind the open invitation of CEO of ICANN to submit whatever questions a team consider being relevant for consideration by European Data Protection Agencies as we go and develop our model or our system, and I always will keep that invitation in mind, and as I already mentioned, one question has bubbled up from our discussion on Tuesday, so maybe that will be not the only one and we will communicate them to you informally but also formally for the record.

So I understand you said that Data Protection Agencies or European Commission will be on summer retreat during July/August, so most likely, we will not get any feedback or update from you prior September. But also, if I may ask to keep us informed on every movement that you spot from the side of European Data Protection Authorities, that we can also factor those movements in our policy considerations.

So may I conclude with these words, or is there any other team member wishing to intervene at this stage? So thank you very much. Thank you, Elena. Thank you, Team.

So we have now on the agenda, the second reading of the case on intellectual property infringement. Since the coffee break is scheduled at 10:15 and now it's already 55, so maybe we will do this the following way. We will listen introduction of staff, Marika, on the changes that have been introduced in the template as a result of a conversation on Tuesday. So Marika will walk us through all the changes that also have been submitted to you yesterday morning. Right? That was yesterday morning. And then we will break and we will resume discussion after the coffee break. Will that be okay? Not to split our conversation in a [few] parts.

So with this, Marika, floor is yours.

MARIKA KONINGS: Yeah, thank you very much, Janis. This is Marika. I think we actually sent this out late on Tuesday evening and I think that's shown as we realized afterwards, there was some duplication in the worksheet that was not intended to be there so we've actually removed that, so the diversion you see now on the screen does not have that duplicate language in there and we've actually already gone a bit further thinking ahead on additional categories that we need to be considered but I think that's something we'll discuss later in the day.

So as we discussed on Tuesday, there was a lot of feedback and input and suggestions from several of you mainly focused on the safeguards and authentication section. So what staff basically did is go into these sections and start applying those proposed changes and suggestions. However, when we were doing that, we realized that the document could actually benefit from a bit of reorganization to really make it very clear to whom these different safeguards are intended to apply or by whom they're expected to be implemented.

So what we did is create, basically, separate categories or entries for the different parties that are expected to meet these safeguards or implement these safeguards. So I think as you look at this version, hopefully, the language shouldn't be too different from what you saw in Thomas's version, but we, of course, have tried to kind of make the language consistent, also to be very specific, for example, on whether it's a requirement or a guidance by using terms such as "must" or "may" and [as that], factoring in some of the feedback that was received during the session.

We tried to do the same thing in the accreditation part, and just maybe taking one step back on the safeguard, so we basically split that out and safeguard is applicable to the requester. Safeguard is applicable to the entity disclosing the nonpublic registration data, and of course, at this time, we're still agnostic to whether that's contracted parties or whether that's in the form of a unified access model with a centralized entity doing the disclosing. Safeguard is applicable to the data as subject and then we've added, as well, a category for safeguards that are applicable to the access or disclosure system.

So in the accreditation of user groups, again, I think this should all look familiar. But what we've done here, we've added this notion of potential development of a code of conduct in which a number of criteria or requirements would be included. So I think those are the main changes we've made. I have to say I was going through this. As the focus of the case changed slightly with the new wording in the title, that there may be further changes that the group needs to consider in relation to the other sections.

As we didn't discuss them, staff didn't feel comfortable in going ahead and making some of those changes, but for example, and as well for the clarity and consistency, for example, in Section C, the data elements typically necessary and I think that's a section we moved up as it seemed more logical to have it higher up there. It's currently written text. This is something you haven't discussed yet. There are still some questions in there that Thomas left, but from a staff's perspective, I think ideally, at the end of the day, we just have here a bulleted list of the data elements that are typically necessary so it becomes easier to review this. But again, this was not discussed yet so we hope that that is, for example, one of the items that can be considered here as the group looks at this further.

And similarly, for example, Section D now has quite extensive text in there but I think the question is that was probably helpful for the conversation here. Is it still required to be in the template or can this just be narrowed down to 61F? And as you'll see as well, we've updated the heading for this section to make clear that this is the lawful basis of the entity that will be disclosing the nonpublic registration data to the requester. So there is no confusion around that.

And similarly, I know I think Alex worked on kind of reframing, a bit, the title of the use case. You may also want to look at does that, in fact, for example, the user groups or the user characteristics, as well as the description of what is expected to happen in relation to this use case?

So I think that's in a nutshell the changes we've made. We know that you probably won't have had much time to review that in detail. As said, we did provide you as well with a redline version, but as we moved around quite a number of sections, it will probably look like more changes have been made than were made from a substance perspective. So we would suggest, and that's what we've put up here in the screen as well, to look at the clean version and I know that we'll soon go to a break. I think the approach, we started off on Tuesday, I think looking at the clean version, having comments and suggestions, and then moved to redlining or looking at what staff was doing in the background to try and capture the changes but I think we quickly got kind of distracted and then too much focus on wordsmithing instead of the higher level input I think that we're looking for.

So one proposed approach would be here to kind of, indeed, take in the input that you have or the suggestions you have. Staff is happy to take that back and kind of have another go at updating this. Of course, if anyone else wants to hold the pen, that's perfectly fine with us as well. But that may be the most constructive way in moving this forward.

I do know. I think I did see suggestions from Farzaneh, I think, go to the list. I don't know if she's online and wants to speak to that when we go to a queue, but I just want to recognize that there was some input already shared and for those that haven't had a chance to look at that, you may otherwise look at it during the break.

JANIS KARKLINS: So thank you, Marika. So what I would like to propose now, please take those ten minutes remaining until coffee break to review individually the text. Then please have a 15 minute coffee break, mingle with the other participants of the meeting in the area where coffee is served, and then please be back in the room at 10:30 sharp and we will start a conversation. I would suggest that we go, I would say, chapter by chapter and see whether we can, we're in agreement what is written in the right square of each of the subgroups. So thank you very much and the meeting will be …

UNIDENTIFIED FEMALE: Janis?

JANIS KARKLINS: Yes?

UNIDENTIFIED FEMALE: Sorry. We actually have a photographer with us in the room, so this is the perfect moment to maybe have a group picture.

JANIS KARKLINS: Why not? And there was Marc. Marc, you want to say something?

MARC ANDERSON: Yes. Thank you, Janis. I just wanted, I thought Georgios made a very good point in chat that we sort of made a great presentation from the strawberry team and discussion afterwards, but we sort of didn't agree on what the next step is. So I think maybe I'd like to request some time on the agenda this afternoon for us to spend a little bit more time as a group talking about that. I think it would be a good use of our face to face time if we could maybe spend some time discussing how best to engage with DPAs, the strawberry team, and how to move forward.

JANIS KARKLINS: Certainly we can. I thought I tried to make a conclusion and proposal, but if that is not enough, I'm happy to entertain and maybe we can chat a little bit during the coffee break to understand what else we could do [inaudible] what I said. But we will come back to this in the afternoon. Thank you.

So group photo.

UNIDENTIFIED FEMALE: So if everyone can basically go on the lefthand corner, from my perspective. EPDP team members and alternates.

[The recording has stopped.]

JANIS KARKLINS: So shall we start? I think we need the recording.

[This meeting is being recorded.]

JANIS KARKLINS: Thank you very much, colleagues. Let us now turn to the use case, which is now displayed on the screen. As I suggested, we would use the method going one section, one by one, and discussing what is written on the righthand side in that [cone].

Since this is the second reading, I think we will be able to go through these sub-sections rather quickly and please, if you want to intervene, raise your hand in the Zoom room. I see Milton is already in line. Milton, please.

MILTON MUELLER: Yes. On the whole, I thought that this document came out quite well. I had a couple of minor adjustments that I'd like to see made. So number one in Section B, why is nonpublic registration data requested?

JANIS KARKLINS: Milton, my apologies. Let us go section by section, and every time, when you want to introduce something, please do it.

MILTON MUELLER: Okay. Are we still on A?

JANIS KARKLINS: No. We haven't started yet.

MILTON MUELLER: Well, I'm starting for you. I'm accelerating the pace here. I'm really gung-ho.

JANIS KARKLINS: But I take note that you want to speak on sub-section B.

MILTON MUELLER: And another one. So I just thought I would –

JANIS KARKLINS: No, no. Thank you. Apologies for that.

MILTON MUELLER: So let us start now with sub-section A. Any comments? Brian.

BRIAN KING: Thank you, Janis. Yeah, we added service providers. I believe we added it below. I think it makes sense to add it here just for clarity. There is some discussion about whether agents captured that, and agents can get a bit legal and might mean different things in a legal context, so just for clarity and for precise language, we should add service providers there. Thanks.

JANIS KARKLINS: So thank you. Staff is capturing all the edits and proposals. So Daniel?

DANIEL HALLORAN: Thank you, Janis. I think that before Section A even, the name of the use case changed from, I think, from trademark owners requesting data to trademark owners processing data. I would think that the trademark owners processing data would be something that happens after the trademark owners actually get the data disclosed to them and then they're processing it later. I thought the use case was more about the issues presented by the trademark owners requesting the data, so I'd propose to go back to that.

JANIS KARKLINS: Okay, thank you. And after you speak, please take your hand down. Alan? Alan Woods.

ALAN WOODS: Just in relation to the word "agents", and again, this comes back to a question that was raised yesterday by Brian or a statement by Brian – or not yesterday, but the last day – we are talking about establishing safeguards as well, even in the user groups. And I'm not jumping ahead, I promise.

But in this one, I think "agents" is a defined term and if it is a more legally defined term, that's even better. This concept of – sorry, what was the service providers? – is a little bit too open and broad. And in this instance we should be defining. We shouldn't be allowing the door to swing wildly in the breeze, so I would be happier with the concept of a more legal defined agent concept.

JANIS KARKLINS: So Brian, would you agree in this particular sub-section?

BRIAN KING: Yeah, partially. I think that leaving it as “agents” doesn’t fully capture the reality that thousands of companies use a brand protection service provider to do this as a practical matter, and so, maybe we could agree more specificity around brand protection service providers, or something more specific. Milton mentioned yesterday in the chat that the Georgia Tech pizza delivery person is a service provider to the company, and certainly, I guess they provide some service. But if we were aiming for specificity, brand protection service providers, I think disambiguates the word “agents” and also reflects the reality of what happens in the industry, that thousands and thousands of companies use service providers to do this work.

JANIS KARKLINS: Thank you. Alan?

ALAN WOODS: Well, that’s our job. Let’s define “agents” then, and [clue] that one. Let’s not open it up. Let’s do the work and define it to include that.

JANIS KARKLINS: So you are in agreement then. Brian?

BRIAN KING: I think so, but I don’t know what Alan is saying, how we do the work to that. So I agree that we can do the work to disambiguate that. Do we want to do that later?

JANIS KARKLINS: So maybe we also need to keep in mind that we’re talking now about specific cases and based on our common understanding of those cases, we will try to extract from them trends, which then would potentially constitute the policy recommendations. So therefore, we need to be reasonably accurate in working on those. But we need not to enter in the wordsmithing and sort of dot-searching exercise. So with that understanding, I will call now on Margie.

MARGIE MILAM: I think we should add brand protection service providers here. I think the specificity is needed, and so I would be uncomfortable waiting to include that later.

JANIS KARKLINS: Okay, thank you. Alan, would you agree? Adding the service providers? Alan? Marika?

MARIKA KONINGS: If I could maybe make a suggestion, would it be helpful to just add a footnote to agents that says something like "including brand protection service providers" so it's clear that they fit within that category?

JANIS KARKLINS: So I see nodding. Yeah, good. We will do that. So may I take then that we are in agreement on Sub-section A?

So Sub-section B, Milton, that's your turn now.

MILTON MUELLER: Yes. Let me just pull up the document here. So this may seem like wordsmithing, but I think it's actually more important. It's kind of responding to Farzaneh's suggestions about what data is actually needed. So instead of saying nonpublic data is requested in order to, we could say it is requested because it is necessary to take legal action against IP law violations, and that just more carefully specifies that you request what you need. You don't just request everything.

JANIS KARKLINS: So thank you. Milton, the reaction to Milton's proposal, Alex? Alex Deacon.

ALEX DEACON: Yeah, I think we're okay with Milton's proposal. I had another suggestion here. Just again, I wasn't too sure how much wordsmithing we're doing here, but just to make this section be consistent with the use case name, I figured we should probably update because it is necessary to establish exercise or take legal action against IP law violations. That was the first thing. Does that make sense? Again, I don't want to wordsmith.

JANIS KARKLINS: I think that would be a little bit too far going in that case.

ALEX DEACON: Okay. Then I have a bunch of wordsmithing nits that I've been working on and I could submit those after the meeting.

JANIS KARKLINS: Yeah, wordsmithing proposals could be submitted directly to staff for consideration. Thank you. Daniel?

DANIEL HALLORAN: Thank you. My question is sort of like Alex's. What's the scope of this? It's talking about trademark infringement generally in the use case and then in this Section B, it talks about IP law violations through the registration of a domain name, which seems narrower, like just talking about cyber squatting. And I wonder cases like a trademark owner are concerned about counterfeit goods, if that would be excluded in this use case. Is that a separate use case? Or is that intended to be covered by trademark infringement generally? Thanks.

JANIS KARKLINS: For the moment, since staff did not have sufficient time to go through and adjust text because of the enlargement of scope of this case, it will be done after this meeting, as the case will be finalized. And necessary adjustments will be made when [inaudible] line, the title which is larger than initial title, with the text of the document itself. Margie, please.

MARGIE MILAM: I think you just hit my issue, so it should track what's on the use case. So it would be nonpublic registration data is requested and then you just track what's in the title, establishment exercise or defensive legal claim.

JANIS KARKLINS: Yeah, it will be throughout the text, not only here but throughout the text where it's needed. Kristina, please.

KRISTINA ROSETTE: Never mind. You all just covered what I was going to raise.

JANIS KARKLINS: Good. Brian?

BRIAN KING: Yeah, thank you. I wonder, and I don't want to go back if we've already decided this but I don't think it's wordsmithing if we update this to establishment or exercise of legal claims, and the reason that we suggested that language is because it tracks GDPR and I think that makes this more legally sound if we're saying this is the GDPR reason why the data is being requested. So happy if we don't agree, but that was the reason and not really wordsmithing.

JANIS KARKLINS: Okay, thank you. So with this, staff captured all the proposals. I think we are on the same page and let us move to Sub-section C.

And here, I would like to suggest that please come up with a very precise formulation data elements that would be needed that would replace the text in the box. Trang, you want to speak?

TRANG NGUYEN: Yes, Janis. I was going to make some suggestion to [distill] that text in the box down to very clearly identify the data elements, and then to help with that as well in the labeling of C, perhaps, we could consider changing the text data elements typically necessary, which is a little vague to something a bit more specific, something like maximum data fields that maybe disclosed in this use case or something along those lines to make it clear.

JANIS KARKLINS: So thank you. We have a proposal to change the title of the box on maximum data elements to be disclosed. So please reaction and also suggestions on those specific data elements. Margie?

MARGIE MILAM: I think we need to add e-mail address and telephone number and fax because since it relates to the establishment exercise or defense of legal claims, a lot of the work that happens before you file a claim is you send a cease and desist letter. You contact them and try to work it out before you actually file a legal claim. So you need to add each of those elements back. Thank you.

JANIS KARKLINS: So proposal is to put five elements, name, organization, e-mail, telephone and fax. Sorry, I'm trying to [inaudible]. So Alan. Alan Greenberg.

ALAN GREENBERG: Thank you very much. The accuracy studies that have been done over the years have shown that there is a very high rate of inaccuracy of contact data in any given registration, and of course, we're removing the administrative field and some of the tech fields so we have a smaller group to work with.

The same studies also show that for any given registration, there is likely some contact information that is valid and usable. So if we're trying to make this really usable, that is, provide information to make contact, we can predict with a high amount of assurance that some of the elements in the registration data are wrong but there's probably something good. So I support Margie's position of basically, if we're trying to enable communication, then really, we need the whole package of all communication fields, all contact fields, to give some level of assurance that we'll be able to make contact. Thank you.

JANIS KARKLINS: Thank you, Alan Greenberg. Alan Woods is next.

ALAN WOODS: Thank you. So I think that Margie, the suggestion to change to the maximum data element, I understand where it's coming from absolutely. I think it might unnecessarily complicate matters in this just purely because, again, when it gets down to the nitty-gritty, and this is why we're talking about the specific use case to see what decisions a discloser would have to make.

It depends on the actual request itself as to what data elements are to be released. So what we're trying to do here is, typically, in your given, this is what we would give. It's not necessarily the maximum that you would give, but that typically makes more sense to me, I agree might be able to be named differently. But we're not always going to be looking at the maximum because it depends on the individual case.

So in that instance, in certain cases, we need to then think of things like necessity of that. So you're saying that you have to have the facts and the phone number, but again, that's this whole typical, as opposed to maximum. So I would just exercise caution on how we are phrasing that because, again, it doesn't apply across the board. So in the concept of the use case, let's be a bit more kind of mean as opposed to max.

JANIS KARKLINS: So thank you. Can we try to adopt, also, in every future discussion, a formulation, something like "not more than" which would suggest that would be maximum, but not necessarily, that we could also, depending on the case, we would go also for smaller version if appropriate. Margie?

MARGIE MILAM: Well, I think, for one, the requester isn't going to ask for those things if they don't need it. But I think we need to deal with the necessity issue. I think they need to say it's necessary. So I don't want to agree that every time it's a trademark issue, everybody gets everything. I mean I totally get that. I think they need to ask for the specific fields and say they need it.

JANIS KARKLINS: So thank you. Kristina?

KRISTINA ROSETTE: Just two broader points. One, I was able to confirm during the break that we did actually define registration data in our Phase 1 final report, so given that it is a defined term as far as we're concerned, I think we need to be consistent about that and also, we don't need to decide this now but I would just flag that we refer in some places to registrant. In other places, to registered name holder. The contracts refer generally to registered name holder, and again, just to flag something that I think if we mean something other than registered name holder, we're going to have to have that discussion or decision at some point, not necessarily now. Thanks.

JANIS KARKLINS: Thank you, Kristina. I think it would be good if we could get on the same page for this specific case, what data typically could be disclosed. And as I mentioned, if we will have a series of cases, then probably that, or that may give us a trend that we could use for a policy recommendation. So I see Marika is next in the line. Marika.

MARIKA MILAM: Yeah, thanks, Janis. One suggestion I had as well, it currently refers to postal address, but my assumption is that we include the data fields that we defined in Phase 1 so it would be street, city, postal code. I just want to confirm that that's, indeed, the group's understanding. And country, but I think that's already published. No? Is it redacted? Okay.

JANIS KARKLINS: No. I think also, what Kristina said, we need to use systematically the same terms referring to the same individuals or the same subject. Milton, please.

MILTON MUELLER: Yes. I just wanted to first respond to Alan Greenberg that the rationale he provided was actually, I think, not legally valid, that it would be convenient or easier if they had all the data elements because one of them might not work. You really do have to make a necessity argument here.

That being said, I think I want to call attention to a tension here in the way we define these use cases. So I agreed when the IPC proposed to broaden the definition of the use case to establishment exercise or defense as opposed to, I think it was just enforcing against trademark infringement. But by broadening that definition, we have also made it much fuzzier what data elements might be considered to be necessary.

So for example, only the lawsuit case, then yeah, you'd pretty much just need the postal address and those fields related to that whereas if you want to do a demand letter or a warning, you might need the e-mail address might be the best way to do that. So the more we broaden the definition of the use case, the harder it is for us to pin down necessity of data elements.

And I think Alan hit the nail on the head here, is it really depends on the specific request, and this is why I think we're going to run into an issue about the automation of responses because of this issue.

JANIS KARKLINS: So thank you for warning us what awaits us at the end of the road. I think with the implementation, we will think as we progress with the policy recommendations. But of course, as always, we need to keep in mind those difficulties or potential difficulties. So next is Margie. Margie? No. Daniel.

TRANG NGUYEN: Thank you, Janis. Dan raised his hand for me. I wasn't in the Zoom room. I am now. Just a note from an implementation perspective that as the EPDP team is discussing what data elements to be included for this particular user case, that it documents the rationale for each of the data elements identified as to why it's needed for this user case, just that it would be helpful to us in implementation to make sure that whatever the policy language ended up being is in line with the original intent of the policy discussions. Thanks.

JANIS KARKLINS: So thank you. Any reaction to proposal that also should be a documented rationale for disclosure? So then I ask staff to capture that element. So any other interventions on that sub-section? So let me then maybe conclude where we got with this. Basically, we felt comfortable with systematically using a term that not more than certain data elements should be disclosed, that the disclosure request also should provide a rationale for request of disclosure, and then that the data elements themselves, which need to be disclosed also would depend on the case. But as a policy element, I think we have enough to process.

So I have two further requests, Marc Anderson, and followed by Margie. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I think what you just said sounds right, but I'm not sure we heard exactly what Trang was saying so I raised my hand to ask her to repeat what she said.

JANIS KARKLINS: Trang, would you be willing to repeat? Please.

TRANG NGUYEN: Yes, thank you and thanks, Marc. What I was just merely suggesting is that as the group discusses and then ultimately decides on what data elements to be included for this particular user case, that it documents the rationale for why that data element is to be included in the policy so that when we actually start to write the policy language, that it's clear.

So for example, I heard mention of a phone number, if that is one data element that should be disclosed, sort of the rationale for why the EPDP team believes that that data element should be one of the data elements that should be disclosed under this user case. I hope that's clear.

JANIS KARKLINS: Alan, is it clear enough?

ALAN WOODS: So just to be clear, what you're saying is that we are going to give an indication for implementation that, sorry, the [inaudible] reason for asking for that telephone should be expected, not that we are going to set the reason for why that particular data element would be released. So the requester would provide that disclosure, not us. Or that rationale, not us.

JANIS KARKLINS: Trang?

TRANG NGUYEN: Yeah, so the requester would have to provide rationale as to why they're requesting. Yeah.

JANIS KARKLINS: Okay, thank you. Margie?

MARGIE MILAM: So I thought when we were talking about rationale, we were talking about it in our report, like why you would have the telephone number in this use case. I wasn't saying we should have in the template rationale for everything. That doesn't what the templates say and I think we've already written the template in Phase 1, is the purpose. This will elevate up to a purpose, right?

So when we finish these user cases, we will have purposes that are authorized and that's what gets cited in the template. So I just wanted to clarify that that was my understanding.

TRANG NGUYEN: Yes. My suggestion for the rationale was to be included in the final report to document the EPDP team's discussions and thinking.

JANIS KARKLINS: So thank you. Dan, you are not convinced?

DANIEL HALLORAN: Thank you. I am still a little bit unclear – I'm sorry – between Alan and Margie. Are we trying to do the work here in this use case, and decide, for example, do trademark owners need the e-mail address of the registrant, or is that going to be decided every time there is a request from a trademark owner on a request by request basis, if that trademark owner needs that e-mail address for that request?

MARGIE MILAM: If I could reply, what I thought we were going to do is say that it's one of the data elements that can be authorized in this if requested. So the onus on the requester is to request the data that they need, and so, I think when we leave this discussion, we should have agreement that the telephone is a legitimate element for this user group, the e-mail, the fax number.

JANIS KARKLINS: No. I think that we can draw a conclusion here. Since we agreed that not necessarily all contact information or all contact fields would be disclosed systematically, so then requester, depending on the case would request what type of information or what type of contact information he would like to receive and would provide reasoning why.

And that is how it should work. I think it is reasonably easy, also, to automate if we get to the automation, just click why, and then you just click on the reason this is why. So again, for this particular case, I think we're fine. We will see how it will be in other cases and see what trend emerges from this conversation. Marika?

MARIKA KONINGS: Yes. Thanks, Janis. I just want to confirm, I think, the way I've captured it because I think we're talking about two rationales in one way. The one is, and I've basically added a footnote to the data elements that may typically be disclosed that basically says that for each request, a requester will need to confirm which data elements are necessary, which I think aligns with what Margie said. And I've also made a note that the EPDP should provide its rationale in its report for why these data elements are typically necessary for this use case because that's what I understood Trang's point to be. So I think hopefully that captured the two aspects, and of course, some further work may be needed once we get to the report stage to kind of define the rationale from the EPDP team's perspective why these data elements are typically disclosed for this use case.

JANIS KARKLINS: So thank you, Marika. Let us move to the next sub-item, and that is D. So here, my question to the team would be whether we would try to display in detail every legal base, legitimate interest in each case, or we would simply use abbreviation, like in this particular case, 61F, and provide then the list of those broader information in the annex or some in an attachment. And I'm asking for every next case, what would be the favored approach. Please, any comments? I see Alex Deacon. Alex?

ALEX DEACON: Well, on your specific question, it seems to me that perhaps we need to go through a few, one or two, maybe three of these before we could determine how to modularize them and abbreviate them, if you will. It may be that the description of 61F in the trademark would be different for cyber security and elsewhere. I don't know. That's my quick response to your question. My hand was up for something else.

JANIS KARKLINS: Thank you. Something else?

ALEX DEACON: Yeah.

JANIS KARKLINS: Please [share].

ALEX DEACON: So my question, [inaudible], is a little bit, is at a higher level. I've been trying to think about how we're going to move forward here and what additional use cases may be required. So this actually bleeds into that agenda item later on, which is to think about what other use cases we'll need to submit moving forward.

61F, I think, is definitely a valid use case, sorry, a valid legal basis for this particular use case, which specifies trademark owners directly processing data in the establishment, etc. The question comes, and again, we'll talk about this later with the law enforcement. There are cases where there's criminal investigations by law enforcement for trademark, for IP issues, and so the question is, is that a separate use case? Or could we, would it fall under this use case, a different requester, law enforcement in this case or a legal authority, and thus, a different legal basis?

There's lots of ways to slice and dice this. And I'm just trying to make sure if there is additional work that we need to do that I have that on my list of things to do. I hope that makes sense.

JANIS KARKLINS: My answer to your question would be let us stick to this particular case and then when we go to other cases, let's stick to a particular case and see whether any trend comes out from, let's say, comparing our views on those particular cases. Margie, please.

MARGIE MILAM: Yeah. My concern with this language is it's only applying 61F and as we've put in our comments before, that there are multiple legal bases that apply here, and we've asked for legal counsel on that.

And that issue is also raised by the European Commission in its letters noting the different legal purposes that may apply.

So I think this is too restrictive and I think we don't need to have that discussion now. I think we get the legal advice and then we go back to all the use cases and work on it. Certainly, 61F is one of them so I'm not saying that 61F is wrong. But I'm saying that there are others that apply depending upon the circumstance. And so my suggestion here, and for all the others is we're going to have to do that analysis after we get the legal advice.

JANIS KARKLINS: Thank you. Daniel?

DANIEL HALLORAN: Thank you, Janis. Responding to your earlier question, I think it would be good for the purposes of the template to try to focus it so if you're asking what's the [inaudible] basis, then the answer for this would be 61F. And I think I'd like to compliment, I think this was Thomas drafted this, and there's a lot of good thinking and writing in there, but it's on sort of other topics. He brings up cross-border transfers. I don't know if that's, it seems like a worthy topic for the team to look, but I don't know if it fits within that 61F section, what [inaudible] basis is. And then he also goes into if you're in 61F, something about the balancing and it seems, I wasn't clear if this template is supposed to be doing the balancing where he talks about in view of the alleged involvement of the registrant and infringement, it can't be assumed that the interests of the registrant outweigh the interests of the IP rights.

So he's talking about the balancing and I don't know if that's something that's going to be done by the team in saying for this use case, the interests of the trademark owner are always going to outweigh the interests of the registrant, or is that going to have to be juggled on a case by case basis? Btu anyway, there are a lot of considerations Thomas brought in usefully, but I think maybe those should be in the template if you need to address those on other use cases. We don't want to just forget it because they're in Thomas's big long essay on this one sell on this use case. Thank you.

JANIS KARKLINS: Thank you. Any reactions to Dan's question? Please think about it before Marika speaks. Marika.

MARIKA KONINGS: Yeah, thanks, Janis, and indeed, as Dan said, it would be good if the [group could] kind of agree what is required in this field. Of course, some additional information might belong somewhere else or may not be necessary, may have been just helpful for this conversation and maybe sufficient to just put the lawful basis in there.

I just wanted to respond to Margie that based on the discussion on Tuesday, we kind of took away from some of the comments made that the group only should focus on the lawful basis of the entity disclosing the information. So that is what is noted here, and then I think for the requesting or the further processing of the data, the requestor will need to identify its own legal basis. And indeed, others may apply there, but at least what I understood from the comments is not necessarily for this group to decide, it's for each requestor to review and make sure that they use the appropriate lawful basis.

And one thing on Alex's point, I'm just wondering as well because indeed, I guess there may be cases where the requestor may have a different lawful basis compared to the lawful basis of the entity disclosing, but I'm just wondering if that might then translate potentially in different safeguards, that that may be the scenarios the group may need to think of if they're – and again, I'm not an expert here, so hoping that others can confirm that, but that might be the place where that would be reflected if there are different lawful bases.

JANIS KARKLINS: Thank you, Marika. Brian?

BRIAN KING: Thank you, Marika, again. Dan, to your point, maybe we add a section, kind of parse this out. I think you're wise to say this should focus on 6.1(f). And the other things that Thomas cites and discusses about Article 21 and 49, maybe go in a section we call supporting authority or something along those lines to further beef up and show that the thought went into this, which the DPAs will want to see.

And then Marika, to your point, MarkMonitor has received legal advice that says that the disclosing party may in fact have more than just the 6.1(f) legal basis. I think that’s the one that we all kind of agree works here and that we should start with, but you're right, it is for the parties seeking the disclosure to come with their own legal basis, but the disclosing party may also be able to rely on some of the others. So I support Margie’s suggestion there that we maybe come back to that later once we get some legal advice from Bird & Bird that the EPDP team can rely on.

JANIS KARKLINS: Okay. Thank you, Brian. Margie, you wanted to speak?

MARGIE MILAM: Brian said what I was going to say.

JANIS KARKLINS: Okay. I have two further requests. One comes from Amr, and then from Alan Woods. Amr, please.

AMR ELSADR: Thanks, Janis. I think Dan's question is a good one, and assuming that 6.1(f) is the legal basis being declared by the requestor, there has to be some kind of balancing test performed to determine whether the legal basis being provided and the reasons outweigh the rights and freedoms of the data subject or the registered name holder or not. So this is something we might want to bake into this kind of use case.

I guess I'm not sure what section we might want to do that in or whether it's part of the safeguards or whether it's a section we might want to add to the use case or not. But thanks for the question, Dan.

JANIS KARKLINS: Thank you, Amr. Alan Woods.

ALAN WOODS: Thank you. Just in relation to both Brian and Margie, and specifically Brian there, I'm not not open to being wrong in this, but I find it difficult to understand what other legal basis is in this particular instance. And Brian, if you're referring to legal advice that you have received as a company, obviously, this question [inaudible] but it would be great if you could share that with us if that was a possibility, of sharing those legal advices with the group. That is a matter for you, but it doesn't really help us for you to say, "We've received legal advice" without actually seeing that legal advice. But then that's definitely something that we should probably ask Bird & Bird very quickly, because again, it kind of somewhat blows my mind to try and figure out how anything but 6.1(f) could apply to this particular use case. I mean we're not taking a legal – or like 6.1(c) or vital interest 6.1(d), but I don't see how they fit into this use case. So I would be very interested to see legal advice on that.

JANIS KARKLINS: Look, we certainly will not ask legal advice on hypothetical cases that we're studying. We're discussing, and we need to assume that this would be sufficient for this particular case in these circumstances for the sake of discussion, go to the next case, see what would be legal basis in that one, and ultimately, after examining a number of cases, try to draw a conclusion what would be the right policy approach in addressing question of legal basis.

So what I heard was that maybe we need to think about legal basis disclosed by or announced by requestor, and that could be used by processor, by CP, to see whether they are in agreement by that stated legal reason.

So I have one more speaker. That's Mark SV, and then we'll move to the next subsection. Mark.

MARK SVANCAREK: Amr, I think that if we're going to be talking about the basis of the requestor, for example if MarkMonitor is under contract to Microsoft to request the data, I think that could be in the safeguards section, but since here in D, we're just talking about the basis of the disclosure, it shouldn't be applicable to the section. This is just the section on the discloser.

AMR ELSADR: Could you just repeat that again?

MARK SVANCAREK: Sure. I thought I heard you say that we should consider the basis of the requestor, and I think you were saying that in regard to the safeguards section. So I was just clarifying that this section D here is about the discloser. So we could revisit that in the safeguards discussion, but I don't think we should discuss it here necessarily.

AMR ELSADR: Okay.

JANIS KARKLINS: So let us move to safeguards section and see whether we can find more convergence and better understanding on this one here. So subsection E. Floor's open. Alan Greenberg.

ALAN GREENBERG: Thank you. And this applies to one of the later sections also. I personally don't have a lot of stake in this game, but I fail to understand why we are limiting it to a single domain name in a request and a single reply later on. If there is commonality – and I'm not suggesting wildcards or anything else like some huge amount of access, but if a requestor has as need to obtain information on multiple domain names associated with the same thing where all of the other aspects of the request are the same, it seems foolish to submit multiple things, and the contracted party have to analyze multiple requests when they could do the job once and save a fair amount of effort in processing the requests.

So I don't see at a policy level why we are limiting the implementation to single names when the logic applies to the same thing and the various parties may well come to agreement that multiple name requests are handleable and generate efficiency on both sides. Thank you.

JANIS KARKLINS: Thank you, Alan, for question. Brian King.

BRIAN KING: I might have the answer to Alan's question. I think if we just add a bit to the parenthetical to distinguish that by the words "bulk access" we mean bulk access as described under 3.3.6 of the RAA, I think IPC could live with the rest of this language about submitting a specific request for each individual domain name.

I don't know if I necessarily read specific request to mean individual or a unique request per domain name. I think specific request for every individual domain name I don't love that wording, but we're not doing wordsmithing here. But I think that captures the concept and probably okay with it.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: Yeah, I would agree with the bulk access concept as long as it's defined by how it was read in the 2013 RAA. That's what we're talking about, and we do need the ability to submit for more than just one domain name, and we don't want to build that into the use case.

JANIS KARKLINS: So, anyone feels comfortable with that reference to 2013 definition? I see nodding. So staff, capture that. Mark SV.

MARK SVANCAREK: In response to Alan G, my first point would be that once we move into a world where this is happening over RDAP, RDAP is set up so that you can only ask for one thing at a time, so that's going to be a moot point. If you need to request data on multiple domain names, which I think was going to be typical in this use case, each one of them will be an individual request to be processed individually by the data controller.

The other point that he made though is that if the data controller prefers in a pre-RDAP world to receive the request in a format such as, "Please send me five at a time" or something, the controller will still have to look at those five and process them on their merits. But if they prefer that they are transported to them in some format, like please send me five at a time or ten at a time, and that is the agreement between the registrar and the requestor, that should not be prohibited. But again, that's in a pre-RDAP world. Once we are in the RDAP world, every request is just going to be one at a time, because that's how it's structured. Thank you.

JANIS KARKLINS: Thank you for reminding all of us about that. Daniel?

DANIEL HALORAN: Thank you. I think items two through four in E are in the wrong place. I don't see how they're safeguards applicable to the requestor. They're more like general features of the system. So I'm not questioning them, just in terms of the template it seems like these are all concepts [we] talk about how the system would work. I don't know why we consider them to be like obligations or burdens or safeguards applicable to the requestor. Thank you.

JANIS KARKLINS: Thank you, Daniel. Any reaction to Daniel's question? Margie?

MARGIE MILAM: Yeah, Dan, I think that makes sense. Actually disagree with my colleague, Mark. Even though RDAP is a one-off answer, the system itself could collect the requests, so the submission side could have multiple requests, and then the system would tee up one off to get the answer. So they're not necessarily the same, and I don't want to limit the requests to one just because RDAP can only do a one-off query. Does that make sense, Mark?

MARK SVANCAREK: May I respond?

JANIS KARKLINS: Yes, please.

MARK SVANCAREK: This was actually contemplated in my intervention, and I'm sorry that it wasn't clear. So I do think that in these cases, typically, there will be more than one name of interest, and they will all be submitted at the same time, but each individual component is going to be a one-off.

So yes, it is likely that at a given time, the registrar will receive a number of these one-off requests, but each one is its own atomic request. They're part of a larger case that is being built, and they with ill all be evaluated in succession, but there's no concept of a wildcard or anything supported in that protocol at this time, and since it's a consensus on how to generate a future version of the protocol, I think it's outside the scope of this. It wouldn't happen.

JANIS KARKLINS: Thank you. Now I have multiple hands, probably in reaction to Dan's question. Alex Deacon.

ALEX DEACON: This is not in response to Dan's question, but I don't have a problem with what he said. Just, again, I have some maybe editorial comments on this section, which I'll avoid for now. I want to address the bulk access issue one more time. We talked about this on Tuesday, that's point number three. And I think assuming that bulk access – as Milton I think helpfully specific that it's referring to 3.3.6, it seems to me that this is functionality that doesn't exist now within WHOIS and won't exist in the future in RDAP. And in any model that we come up with, it seems to make sense to me that it can be deleted. So I'd like to suggest that.

JANIS KARKLINS: Okay. Thank you, Alex. Alan Greenberg.

ALAN GREENBERG: Yeah. Thank you. I just wanted to further clarify, the issue is not in a pre-RDAP or post-RDAP world that I was making reference to. There are some people who believe that these requests are going to have to be looked at manually or to make sure to analyze each of the ones, and I was simple suggesting that a message conveyed one way or another that these seven or 100 requests are all structured identically with the exception of the name will minimize the amount of work that has to be done, and to the extent that we can do that, I think we should. That's all. But again, I have little skin in the game. If people on both sides of it don't care, that's fine.

JANIS KARKLINS: Thank you. Georgios?

GEORGIOS TSELENTIS: Just want to make an observation regarding the [inaudible] because we have three categories of the safeguards. I don't know if it's wise to make it now or later on, because we have safeguards applicable to the requestor, to the entity disclosing, and then we have safeguards for the data subject.

I think the issue here is that all the safeguards refer to the data subject. The way we have put in the template is who applies those safeguards. [It] safeguards actually for the data subject all three categories. So I don't know, maybe I can wait later on when we go to the third category, which is to the data subject.

So it's probably a question, who applies those safeguards in each one of these categories? Because they all refer to [inaudible]. Just to Marika also for the way we structure the template. Thanks.

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

TRANG NGUYEN: Yes. Thank you, Janis. I have a question about item number five here. It says that the requestor must provide representations about how they would use the requested data and then that will be subject to auditing. I have a question about the word "auditing" there. What is meant by that? Who's going to be doing the auditing, for what purpose, and then what would be done by the findings of such audit? So maybe a little more clarity around what is meant by auditing there would be helpful. Thank you.

JANIS KARKLINS: So, is anyone willing to answer about auditing? Milton?

MILTON MUELLER: Yeah, I think that's asking us to go too deeply into implementation. The point is that there will be oversight into the compliance or the conjunction between what you're saying you're doing with the data and what you actually do with it. How we work out that auditing is not appropriate for this particular template.

JANIS KARKLINS: Okay. Thank you. Let me return to the list. Alan Woods.

ALAN WOODS: Thank you. So just in relation to the bulk access, number three there, to be perfectly honest, I don't know how it slipped into a question about whether or not the technology can support a bulk access or not. That's not what this is stating. And in a way, Alan, I think you were actually hitting the nail on the head. This is what this is saying, is each individual request and each individual release of data relating to a particular domain name needs to be reviewed, and you're taking that extra step forward saying if it is identical in form for each one of these tests, can they just be submitted as a whole?

And I don't think we're anywhere near coming to that conclusion yet. We don't know. We need more legal certainty, to be perfectly honest, on that one. But we cannot be seen to be taking shortcuts on that, and that's what this means. It means that each individual request for a domain name's registrant data must be seen to be somehow considered on its individual merits.

Regardless of the fact that there might be 200 and they're all the same, each one must still go through that process of consideration, and we need to be clear that we're not deleting that concept of no bulk access. A single decision cannot issue for

200 domains. 200 decisions will have to issue for 200 domains, and that, I think we need to be clear on.

JANIS KARKLINS: Yes, please, Alex.

ALEX DEACON: Thanks. Just following up on that, yeah, I don't disagree. I think three is an important concept. My earlier intervention was that we delete the parenthetical no bulk access, I think. I'm not suggesting we delete the whole thing.

JANIS KARKLINS: My suggestion would be to look also to F and G, and not just concentrate on E as we're spending a lot of time here. So I think we are in agreement that there should not be bulk access as such, rather, each request should be examined individually. But let's also see how that principle would apply in other cases and see whether that is a trend that would find reflection in a policy recommendation.

Is there anyone – I have literally ten requests for the floor now. Is there anyone who insists on speaking on E, or can we move to F? Margie.

MARC ANDERSON: I'm on E.

JANIS KARKLINS: Okay, then I'm going through the whole list. But maybe – so I see some hands have disappeared. If you do not [insist,] please take your hand down. But if you insist, keep your hand up. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I guess I hesitate to bring this up, but it seems that some of the things we're discussing aren't really safeguards applicable to the requestor. And I hesitate to bring this up because I think what we're discussing are good topics that need to be covered, but it doesn't seem like we're categorizing them in the right place. So I guess, I think we need a little more clarity that section E is safeguards applicable to the requestor themselves, which I took at least to be more terms of use-type safeguards. If I'm wrong on this, I'd love to be corrected, but I've been a little confused about some of the topics we've had under this category.

JANIS KARKLINS: Thank you, Marc. Milton?

MILTON MUELLER: Yeah, just wanted to express opposition to deleting the parenthetical no bulk access. I understand the argument that it's not as easily possible under RDS than it was with the old system, but if that's indeed true, then it has no harm for having that in there. And if some kind of workaround could be done in which you might actually recreate bulk access in some way, I want that safeguard in there.

JANIS KARKLINS: So it's noted, Milton. Alex?

ALEX DEACON: Yeah, I guess just to quickly respond to Milton, as long as the definition of bulk access – I notice there's not a footnote on this bulk access, there's one down there, it's specific to 3.3.6, and I think I may be okay with that.

The issue that I wanted to raise was on four. And I'll note that technically, there are ways to discover where to direct requests kind of automatically that happens today with port 43 WHOIS with the referral. It can happen in RDAP moving forward. So it's not too [sure.] It's really up to the requestor to figure out where to send this request. I think the technology that's being developed kind of handles that on behalf of the user, points them in the right direction.

So I'm not too sure four is necessary, or perhaps I'm just not understanding the reason why – and unfortunately Thomas is not here – four was added. Thanks.

JANIS KARKLINS: Thank you. Margie.

MARGIE MILAM: This is in response to Alan's comments, because I don't think we agree with what you were saying, that each request needs to be specifically reviewed. The point of this is to create categories of user cases where it's possible to have automated responses, and that's consistent with the European Commission letters where they're saying they want this predictable, scalable system.

So you asked if someone disagreed. I don't want to leave that out there. And this is where we're asking for legal advice, whether that's possible. And I think where you're headed is you don't think it's possible. But if we get legal advice that says that you [can] have automated responses with certain categories of user groups, then that makes a feature that we can build into the system. So I can't leave that out there as something that suggests that nobody opposes that view, because I think that's where we're looking at it from our perspective.

JANIS KARKLINS: So, thank you. Alan, please.

ALAN WOODS: Thank you. Single-line response to that is all those letters, of course, do say subject to applicable law, and that's what we're talking about. So I agree. Yes.

JANIS KARKLINS: I will take two further comments on this, and then we will move further. From Amr and Hadia. Amr, please go ahead.

AMR ELSADR: Thanks, Janis. Revisiting Milton's response to Trang a little earlier on five, we had a really quick chat here, and I think Dan and Trang are asking really good questions today and I hope they continue to do so. And we might not need to answer this now, but I think it might be worthwhile for us to at some point explore whether we can give implementation advice to the IRT's eventual work on how auditing is conducted by whom and then what kind of representation of use of the requested data is – how it's done.

So let's not dismiss Trang's question for now. Let's try to capture that if possible, and maybe revisit it at a later time. Thanks.

JANIS KARKLINS: Thank you. And now Hadia.

HADIA ELMINIAWI: Thank you, Janis. I tend to agree with Marc Anderson that the title of item E is a little bit confusing. [It's more terms of use.] I also don't see that item number four belongs there. And in relation to what Margie and Mark were saying, well, we saw in the demo yesterday that you can actually submit more than one domain name at a time, and each domain name is processed individually. So it is possible to have every individual domain processed individually though you actually submit them together. That does not mean that they're all processed together. Thank you.

JANIS KARKLINS: Thank you, Hadia. And very quickly, Brian.

BRIAN KING: Thank you, Janis. Very quickly, I spoke with Thomas about four, and apparently this came from a concern before we were aware of the relevant technology about how requests might be facilitated between registrars. And then I would also support Amr's point to Trang's question about auditing. We're interested in the outcomes of those discussions. Thanks.

JANIS KARKLINS: You know, I think that auditing is on our list of points we need to discuss and come up with a kind of policy suggestions as we speak.

So I have next – I want really to move to the next point, but I see David Cake.

DAVID CAKE: And it really was just a point of clarification. The issue here is not that multiple requests being done quickly or submitted at the same time. It's that the legal decisions are Individual for each one, and the whole process is followed for each one and there's not a bulk process, and they're all justified.

We're not trying to say it has to be slowed down with every decision must be individual and follow the full process. It doesn't matter if those individual decisions a are few seconds apart or a few hours, but each one, the full process is the issue here, not speed of implementation.

JANIS KARKLINS: Thank you for comment. Mark SV.

MARK SVANCAREK: Thank you for that clarification. I think the confusion arises from the fact that we're discussing it in section E which his about requests and not discussing it in section F which is about disclosure. If that comment were in F regarding disclosure, I think it would be super clear. So the question comes up because it's in E, which is why I keep asking transport questions.

JANIS KARKLINS: Okay. I think we need to stop here and move to other sections of safeguards, namely F, and then G. And then we will see how the conversation on safeguards will go on other cases and see what trends emerge from that.

So with this, I open the debate on subsection F, and I will ask Rafik to step in for three minutes on my behalf.

RAFIK DAMMAK: Thanks, Janis. So we have Alex, and then Dan.

ALEX DEACON: Thanks. I think my only thoughts on this section, F, is on three. There's clearly – any service needs to ensure they're operationally protected from denial of service attacks and so on. I think that's a given. I'm not too sure we have to say that in this policy.

This does seem to indicate that there could be rate limiting around requests of an "Abusive nature" for some definition that's not clear. If the assumption is that requests or requestors are identified and authenticated, that they're perhaps also authorized and they have a well-formed request, it’s not clear to me that there would ever be a case where there is kind of abuse on the volume level.

So it’s clearly a gray area here, but I just want to make sure we don’t end up in a situation where legitimate requests are being rejected because of some notion or an indication that they may be abusive, above and beyond of course DDoS and kind of lower-level attacks that may happen on any service. So that’s my concern. Thanks.

RAFIK DAMMAK: Okay. Thanks, Alex. Dan?

DANIEL HALORAN: Thank you, Rafik. And I want to thank Amr for the positive feedback first that he gave to me and Trang. I want to stress that we’re here as we’re supposed to be doing in the charter trying to raise implementation concerns. We’re not taking sides. So every time I'm raising my hand or asking a question, I'm not trying to take one side or the other. We’re stressing – agree with you 100%, and you brought it up earlier, we don’t think – ICANN Org does not make this policy. We’re here to help you make the policy. We’re not taking sides. So don’t take any of my questions wrong, or our suggestions. Just trying to help improve the text and make sure it's implementable.

On F specifically, I think we have a concern about F2 as it is on the screen. It seems a little bit vague and ambiguous. I'm not sure why it's a safeguard applicable to the [inaudible] disclosing the data. Says, "Must return current data in response to request."

I think this is talking about what I think would be a feature of the system, that it's not a WHO WAS system, it's a WHOIS system. It's about current data, it's not supposed to be built to get old data. I don't think we're trying to say that – first of all, when you say they must return current data, it's not that they must always return data. It has to comply with the system and follow all the procedures. So anyway, I think we moved that down to a feature of the system, that it's only about the current registration data. And also, I don't think it was intended to be something saying that they have to return something other than what is the active current registration data. It's not that they have to go check it or verify it or update it or something like that in response to a request. Thank you.

JANIS KARKLINS: Thank you, Dan. Alan Woods next.

ALAN WOODS: Thank you. Just in response, Alex, to what you're saying there. Let's call a spade a spade. That's not necessarily what three is saying there. What three is saying is that the system should not be used for phishing expeditions. I understand the technical safeguards that you're referring to, and perhaps we can pull them out separately.

And I don't think it should be a given. If we're talking about the system, we should state that a safeguard is that it must be sufficiently technologically safe to prevent breaches and prevent lack of access to requestors and things like that. But what that's saying is phishing expeditions should not be allowed and encouraged by the system. That's the way I read it.

JANIS KARKLINS: Yes. Alex.

ALEX DEACON: Thanks. I think that's helpful, Alan. Again, I'm concerned about definitions. What do we mean – I think we can guess what we mean by phishing expeditions, or what it says here, request of an abusive or illegitimate nature.

It's just these are very wishy-washy terms that maybe we just need to be more precise. I agree that the system – and I think by the end, it'll be very difficult to use the system for phishing expeditions. I just want to make sure that we don't unnecessarily block legitimate requests, or build a loophole into the system that will allow for the blockage of these legitimate requests based on some vague notion of phishing or abuse. Thanks.

JANIS KARKLINS: Thank you. Kristina.

KRISTINA ROSETTE: I hate to even say this because it makes my head hurt, but to the extent that when all is said and done and we have a policy and a system, if ICANN Compliance is going to be including audits of contracted parties' compliance with the system, can I just say that we're going to have to put markers down, placeholders for now? Because I think we're going to have to give some real thought to what additional safeguards we may need in order to be able to respond to those types of audits in the manner in which ICANN Compliance has historically expected us to respond to [RDAP] requests. Thanks.

JANIS KARKLINS: Thank you. I hope staff captured that. Margie.

MARGIE MILAM: Yeah, the language in four is a relic of the old system. It's a relic of abuse that we saw in port 43. So I understand where it came from, but I think we're building with the safeguard – I mean I think exactly what you guys said, that we're going to have to go back and make sure we've got the right safeguards up. And we'll do that as we evolve this.

So I just think that that language is probably not applicable, and especially the high volume is an area where I think we spoke about yesterday that we don't want to have an arbitrary limit on the number of legitimate trademark-related cases that we are looking at. So I just want to clarify that the volume issue is particularly problematic.

JANIS KARKLINS: Thank you. It seems to me that we need further discussion on safeguards in a broader context of different cases. I would think that if the European data protection authorities will confirm that requestors are equally liable for submitting their requests in the framework of GDPR, in the context of GDPR, so then prior submitting bulk requests or requests they would have done in pre-GDPR era they would think twice.

So there will be also some natural balancing effect if liability will be split to different actors in their respective way. So I have a few further [requests] on this subsection F before we move to subsection G, because I would really love to get through this document by lunchtime, if that would be ever feasible. Mark SV followed by Marc Anderson.

MARK SVANCAREK: I had a clarification of something that Margie said, and I wanted to ask Kristina for some more information about her very interesting point.

The first clarification was – because [this could be] specific. So Microsoft has many attractive trademarks, and people do infringe them, and we have so many that we hire a separate company like MarkMonitor to take care of that, and MarkMonitor has many clients who are like Microsoft, so in aggregate, MarkMonitor could be making many requests, each of them appropriate and lawful, and we would like to get some certainty on how that would be treated by a registrar who is in an unfortunate situation of receiving a bunch of these requests all at once.

So clarity on this rate limiting stuff would be desirable. And second, Kristina, you said it makes you sick to even raise the question. It makes me sick to ask a clarifying questions about your question, but I'm really ignorant about how what you said applied to this. My first impression was, is that a separate use case? Do we need to turn that into a use case and evaluate it, or is it directly related to one? And if it is, could you please explain? Because I'm really dumb about it. Thank you.

KRISTINA ROSETTE: It's both. It's both kind of a general, which could go into an overall bucket of requirements that apply regardless of the use case, but it also potentially could be requirements that would apply to this specific use case, and that's, I think, part of the problem, because so much of what ICANN Compliance's role in this will be with regard to registries and registrars depends in large part on what we actually end up having.

My point really was more of I think we need to just put a placeholder down that we need to ensure that whatever safeguards, requirements, whatever we're going to call them, for each individual use case and across the system, are such that if a registry or registrar is going to be audited because ICANN Compliance on the basis of that entity's compliance, will they even be in a position to respond? And that's part of the reason it makes my head hurt, because it's a lot of, "If, then, if what," all of that.

So my point really was I don't want us to get to the point where we're like, "Okay, we're done and dusted with this one," and then have to circle back. I just want a placeholder.

MARK SVANCAREK: Thanks. That helps.

JANIS KARKLINS: So thank you. Marc Anderson.

MARC ANDERSON: Thanks, Janis. I know you're trying to get us moving along so we can get to lunch, so I'll try and be brief. Just back on F though, I'm not exactly sure where we left things on the safeguards that are applicable to the disclosing entity. And I heard Alex and Margie’s points about those safeguards shouldn’t be used or abused in a way that prevents legitimate access requests from going through, and that’s a fair point and I agree with that.

But I want to make sure we’re not taking that too far and removing those altogether. I'm not quite sure how staff captured that, but the disclosing entities still have an obligation to protect their systems and the systems with PII.

So I want to make sure we have a balance there. I get the points that they made, but we still need to protect our systems. So maybe we can look at that language further offline, but I want to make sure that that’s not lost in the editing.

JANIS KARKLINS: Yeah. I would really like to propose to go to the next subsection. It is clear to me that further reflection is needed, and I would think that discussion on safeguards on other cases would bring us closer to common understanding. I see Marika is asking for the floor. Marika?

MARIKA KONINGS: Yeah. Thanks, Janis. For now, we've kind of just put in a note that there may be a need for the EPDP team to further define and clarify, especially relating to abusive nature on number four. I'm indeed not exactly sure where the group sits, so it may actually be really helpful in the lunch break, I don't know, maybe Brian and Mark sit together and see if there's a way to come up with language that meets both your needs, because I think staff is not exactly sure here where we should take that.

JANIS KARKLINS: So, shall we move to G? Hadia?

HADIA ELMINIAWI: My comment is with regard to item number three, which says not to be subject to a decision significantly affecting them.

And I would like to refer to article 22 of the GDPR which speaks to automated decision making, and it says which produces legal effects concerning him or her or similarly significant. So to just put it as to a decision significantly affecting them is quite loose. I think it needs to be more defined, and it is defined in the article.

My other quick comment would be that actually, it is possible for the data subject to be – it says here on an automated processing of data, unless this is authorized by law providing appropriate safeguards.

Well, it's not only unless it is authorized by union law, but it's also according to the article, if it is necessary for entering into or performance of a contract between the data subject and the controller, or if it is based on the data subject's explicit consent.

So there are other two possibilities other than law requirement. Thank you.

JANIS KARKLINS: Thank you, Hadia. For your comments. Trang, please.

TRANG NGUYEN: Yes. Thank you, Janis. I think [G] seems like a mix of a number of things. Some of them seem to be related to data subjects under GDPR, and some of them seem to be what looks to be more like requirements like some in the chat have said, rather than safeguards. So I wonder if it's possible to be more clear in the items that we put into this box to maybe highlight what is a policy defined as requirements for the data subject, and then perhaps consider whether or not the elements that are already rights that are provided to the data subjects under GDPR should be included or not included. Thanks.

JANIS KARKLINS: Thank you, Trang. León?

LEÓN SANCHEZ: Thank you, Janis. [inaudible] safeguards [applicable] to data subject, I see that many of the concepts that we're putting here are actually built into GDPR, so these are legal concepts that we will need to respect regardless of having them built into our policy. So for me, it's a bit redundant to be discussing this as we already have this in the law.

So I agree that maybe not everything is in there. Alan, I'm seeing your face, but what I would like to prevent is to go into a redundant discussion of things that we need to comply with regardless. So we need to make our policy complaint to GDPR, but that doesn't mean that we need to build GDPR into our policy necessarily.

JANIS KARKLINS: Thank you, León. Alex, please.

ALAN WOODS: Alan Woods for the record very briefly. I see what you're saying about the redundancy there. However, Article 25 is 100% in play here. We need to do privacy by default, and we can't just [pay] saying "Obviously we're subject to the law, therefore we're going to do that."

The safeguard in the system is insuring as we are creating the policy and trying to define what this will look like that we build into the process everything that means that we can adhere to those specific rights that the process is created based upon those rights, and they are in their own right a safeguard then.

Yes, they are required under the law and my hand went up because of what Trang was saying, but these are the safeguards that we must build into our system in order to tick those rights as opposed to just saying, "Well, of course we're going to apply them because they're in the law."

LEÓN SANCHEZ: To that end, I agree with you.

JANIS KARKLINS: Thank you. Brian.

BRIAN KING: Thanks, Janis. I agree with my colleagues, and I'd say that to expand on what Alan said, I think it might be good to use these as an opportunity to show our work and show that we know about the safeguard and here's how it works in the system. I'd say that applies to one, two, four and five, and I don't think it applies to three. As I understand GDPR, three pertains to the ability to get a bank loan or to get a business license or something like that, or the denial of that based on automated data processing about the data subject's personal data. And that's not what we're doing here. So I don't think that applies to this particular – the law obviously applies, but that specifically, I don't see being relevant to our work. Thanks.

JANIS KARKLINS: Thank you, Brian, for comment.

CHRIS LEWIS-EVANS: Georgios is having a problem with Zoom.

GEORGIOS TSELENTIS: Sorry, it was a problem, I couldn't connect to Zoom. I just wanted to say here – and this was related to my earlier comment – that the previous categories were talking about safeguards and were saying who is going to apply those safeguards.

Here we are talking about something which I agree is inside the law, and probably, the wiser thing would be to move those by defining when we say for example the [inaudible] request confirmation of the processing by saying who is going to provide this safeguard, and move it to the requestor, the appropriate category.

So I think – and by doing so, then we put the liability the [inaudible] has provide the safeguard is specified party in this process. So maybe there is a need for further working out here of those safeguards, because all the safeguards at the end of the day refer to the data privacy and data subject. So maybe there is a little bit of work on the template. This is what I said in my previous intervention.

JANIS KARKLINS: Okay. Thank you. I have two further questions [in this section,] and that is from Margie and Dan. Margie, please.

MARGIE MILAM: I think I agree with a lot of people have been saying, that if it's included, it doesn't seem like it's actually tracking GDPR word for word, and so we'd have to be very careful to do it. It sounds like we're saying, "Don't include it like this, deal with it separately." So I think we probably just need a separate day or whatever where we talk about this and flesh it out.

JANIS KARKLINS: Thank you. Dan.

DANIEL HALORAN: Thank you. I think I agree with what everybody said. We should be focusing – these are rights of the data subject, and that's fine to list them, but we should be focusing on what requirements are we putting on the system, on registrars, on the requestor, who must do what in order to respect these rights in the system. So focus on the requirements, not just the rights and the safeguards.

JANIS KARKLINS: Yeah, and that probably could be done either by putting another column here talking about who would do that, or putting responsible parties [in the records after.] Probably that would be one way forward. Milton, you're the last one.

MILTON MUELLER: Yes. I have no problem with more closely mapping these data subject safeguards to the system requirements. That's a good idea. But I totally oppose getting rid of these or shuttling them off to another part of our process. I think this has to be very explicit and upfront, and we do need to think about what are the system requirements for actually implementing these.

JANIS KARKLINS: Yeah. I think that the safeguards is important part in the template, on every case, and we need to go through all of them, though it's as bit time consuming. Nevertheless, it is necessary to understand better where this balancing point stands.

I would really like to move now to point H, but I have Hadia and Ayden. Hadia, please.

HADIA ELMINIAWI: To Brian and Georgios' point, I think somewhere, we need to put the need to implement suitable measures to safeguard the data subject's rights. And whether that would be done by the controller, if we say the system, then who's really running the system? But anyway, yes, there should be a clause that says that measures should be taken to safeguard the data subject's rights. Thank you.

JANIS KARKLINS: Thank you, Hadia. Ayden?

STEPHANIE PERRIN: Thanks very much. Stephanie Perrin for the record. I was – and I apologize for not having been here at the opening session, but I'm picking up on what Alan Greenberg was saying in terms of parallel processing, and as I listen to all of this discussion on bulk and all of the different aspects of this, this is all part of a risk assessment. So, is there a parallel risk assessment activity going on as we are doing this? It's similar to doing a data protection impact assessment prior to, but I understand that it's an evergreen process as you go along. But that doesn't seem to have surfaced materially in our discussions, so just a question to ICANN Org.

JANIS KARKLINS: Well, ICANN Org is thinking about the answer. Milton, do you want to intervene, or is that your previous hand? Old hand, so to say. Old hand. Please take it away. Dan?

DANIEL HALORAN: Thanks. I'm not sure I caught exactly the entire question. Maybe we should take it on notice.

JANIS KARKLINS: Stephanie, could you repeat –

DANIEL HALORAN: We're not doing like a shadow data protection impact assessment as you guys are working. I think that's work we'll need to do later as a team, or we need to discuss what kind of assessments are going to need to be done, the role of this team, and maybe outside counsel and Org. So we're open to your questions and suggestions on that. Thanks.

JANIS KARKLINS: So Stephanie, maybe you can clarify your question. But I open now subsection F, because it is about also bulk access, and other things. I understand there was already exchange on Tuesday, and it would be kind of a repeat. If that's needed, let's do this repeat. Please bear in mind that subsection H and I stands between you and the lunch which is already there. So please keep that in mind. Lunch can wait. Stephanie.

STEPHANIE PERRIN: Just to clarify the question, Alan Greenberg mentioned this morning that he was perfectly comfortable with doing the Technical Study Group scenario, because he had done a lot of systems work and it was always a bunch of parallel processes. I'm condensing that for the purposes of brevity.

Now, one of those processes that should be going on ongoing in the background is the risk assessment. So, is there a risk assessment team – and I would presume that that would be under Mr. Crain from whatever unit – technical – that he would be in charge and there would be a team assessing the technical risk of bulk access, different interfaces, how this works with a small registry, how it works with a big registry, because to be blunt, in our data protection office in Canada, one of the first questions you're going to ask is, "Where's the risk assessment?"

And if there is no risk assessment, then you're going to say, "Fine, please do the risk assessment and come back." You're not going to get an assessment on liability if you don't know what the risk is. And the whole point of having liability in there is to compensate when there's a breach.

JANIS KARKLINS: Dan?

DANIEL HALORAN: I think I understand the general concept, but we have not bothered John Crain with this yet. I think he would get mad at me if I brought it to him. He would say, "What are you talking about? Risks of who?" I think we need to get further down the road. We don't know who's going to be handling this data, if it's registries or registrars or some central system. I think we need to put more on it before we can start talking [to technical and legal] about what the risks would be.

JANIS KARKLINS: So maybe you can arrange John talking to Stephanie and then thresh out that question. So I have one hand for H subsection, and that is hand of Alex Deacon.

ALEX DEACON: Yeah. Thanks. On H, the first one, on Tuesday I raised a concern about this point and I took an action to kind of formulate my thoughts and pose new wording.

As someone with a technical background versus a legal background, I'm always concerned that setting policy that may unnecessarily limit future innovation and functionality.

I'd still like some time and have an action to look deeper into this, and hope I could send my thoughts and suggestions regarding updated language and wording to the list as soon as possible. Thanks.

JANIS KARKLINS: Thank you, Alex. Any further comments on subsection H? If not, then let us move to subsection I on accreditation. Any comments? Dan?

DANIEL HALORAN: Thanks. We thought the name of the section, accreditation of user groups [inaudible] policy principles was kind of vague. We had suggested wording something more like eligibility criteria for accreditation of this user group. And then there's a lot of language in there about code of conduct, which seemed like it would fit more back up where we're talking about safeguards applicable to the requestor maybe, or whenever we come up with requirements there as opposed to – we didn't see how that related to accrediting – the question is, is accreditation of this user group required, yes or no? And this is code of conduct applicable [to that] user group, which seems like it would go in a different section. Thanks.

JANIS KARKLINS: Thank you. Brian King.

BRIAN KING: Thank you. We have a number of comments about this one. It would be helpful to know what the group is thinking about evidence of ownership of IP rights as a first point. As a general point on this section, I think I'm still interested to know what we're hoping to accomplish by accreditation. As the IPC has mentioned all along, we're absolutely in favor of the concept of accreditation. I'm just still unfortunately not clear about what that does for us.

We know that that alone doesn't provide a legal basis, being a member of some group, so I think we could use more clarity there. And then I really want to caution us about the use of the word "code of conduct," not just because it also means something specific in ICANN land, which I think is helpfully noted in the footnote, but that a code of conduct has not been done before as defined in the GDPR, and I'm not willing to say that we'll wait until that is done here.

We don't know what the DPAs will say, we don't know what kind of engagement we'll be able to achieve, we don't know that we'll get one approved. So that's going to be a prerequisite. That's not going to be something we're able to sign on to.

If the concept that we're thinking about there is a data processing agreement or terms and conditions of using the service or terms of using the data, absolutely, let's call it that to disambiguate this concept, and let's go from there. Thanks.

JANIS KARKLINS: Thank you, Brian. I think that we need more discussion on accreditation. This is a new topic that has been introduced because when we're going through cases, we need to cover every possible topic in each case in order to extract those trends. So the one option is that we use this accreditation in order to facilitate work on disclosure by disclosing first and foremost to accredited entities or individuals. So again, whether that is the case or not, we need further discussion. And if we agree that accreditation is needed, what type of accreditation modalities, who does it? And there are multiple options that may be considered.

So with this, I have next hand up, and that is from Volker.

VOLKER GRIEMAN: Yes. Thank you, Janis. Accreditation, I think before we can answer the question of whether it's required or not, we first may need to be very clear about what accreditation actually means, what is required for accreditation, what accreditation actually gets you, and I think it will also be different from user group to user group.

For example, certain user groups that have certain legal rights to access certain data [or request to store] certain data, for example [competent] police authorities might have such a right under an investigation. They might not need accreditation because they are basically – would be accredited under their own principles, under their own statues already.

So we first need to define what this means, what we want to get out of accreditation, and what accreditation basically provides for that would otherwise be required to provide [inaudible] each and every single request, I think.

The easiest proposal for accreditation would be that it just simply simplifies the request process by not always having to provide the same information, only doing it once, and then being accredited or certified or whatever, and whatever that means.

So let's first define what we mean by this before we say whether it's required or not. Thank you.

JANIS KARKLINS: Thank you, Volker. Margie?

MARGIE MILAM: I agree with the comments about the code of conduct, and I think we want to make sure that we're not limiting how the intellectual property rights are to be evidenced. In other words, they're common law trademarks as an example. So I think that that's something that needs to be considered.

And with regard to the individual requirements versus number two, only issue disclosure requests with respect to trademarks where ownership is evidenced. I think that's a remnant when this use case was only for cybersquatting. So I would suggest deleting that. Thank you.

JANIS KARKLINS: Thank you. I do not have any further requests. Volker is still keeping his hand up, but actually, hand should be down. So I will maybe draw a conclusion to this conversation. Please think about accreditation in a broader sense, also for future conversation. There is probably good reason to think in terms of a system of accreditation, which would facilitate life to contracted parties in order to process all the requests for disclosure of information.

Modalities of accreditation can vary enormously, so we can think of for instance in specific cases of intellectual property, we can think of accreditation done by authoritative international organization like WIPO for instance, or we can think of creating a special accrediting body, whatever that means, who does accreditation of all kinds, independent accrediting body. We can think of many different options, and since we're really at the very early stage of reflection on this issue, also some side conversations probably would be very helpful in order to develop our own thinking in this respect.

So we are at the end of second reading of the document. I think it gave us some understanding that many things still need to be considered. I hope that staff captured sufficiently the ideas that have been expressed and we'll try to reflect them in the next iteration of this case study.

We do not need really to get full agreement on everything, and I will suggest that for the moment, we would park this particular case. We would of course publish the updated version of the case for everyone's knowledge. And we will go to the examination of next cases. And we would return to any specific case as needed in the future. But I hope that going through other cases, we will try to extract those trends and [foster] commonalities on different subjects that we're talking.

So with that understanding, and that would be acceptable to all, we would break for lunch. We have about 45 minutes for lunch, I think that's good enough. And we would return at 1 PM with launching of the next case on law enforcement, and we would listen general presentation of Chris Lewis-Evans, and then Georgios, before getting into detailed subject on the case in general terms, because we do not have sufficient time to go subtopic by subtopic, most likely.

So with this, I was asked to say that the lunch is for team members only, and if something left over, then for the rest of the present in the group, but please, team members, the lunch, I understand, is there. And please return to the room at 1:00 PM for continuation of our conversation. Thank you very much, and bon appetit.

So, guys, we will go in maybe three, four minutes from now.

Thank you very much for starting recording. Folks, we are now ready for the next case study, and that will be on law enforcement. So public safety. And I will ask now Chris Lewis-Evans to make introduction of the case, and then I understand that Georgios will come to speak further after you. Or you will cover both topics? Okay. So Chris, please go ahead.

CHRIS LEWIS-EVANS: Thank you, Janis. So kind of just bringing up the diagram which we've not shared with the group yet, but obviously, this will go on out after this. When we were thinking about how to fill out the purpose/user case for the law enforcement agencies and all the other aspects that we might want to cover, how can we do this properly? How can we formulate this stuff? There was a lot of drawing on napkins, scraps of paper, bits and pieces, and we did think about photocopying and getting it out, but luckily, we got someone that can draw some pretty pictures, and hopefully represent our thinking and how we framed our discussions to actually get through to producing the framework for the user case.

So I'm going to start from left to right. Initial request comes in, and realistically, what we're thinking about there is what's applicable to that, what are the safeguards. So with that, the request itself is going to have to have its own legal basis. There's going to be some form of rules that the requestor is going to have to follow, so that's into the safeguards section that we've just been covering.

Do they need to be accredited? Is that applicable all the time? So obviously, at the moment, without an access model, and if we decide not to have an access model, accreditation doesn't make sense. But if we were to have one, then there would be the need for some accreditation. And then authentication comes into the purpose and the user case, and everything else.

And then obviously under that, have the purpose itself, what the user case is, what records we're requesting, what are the relevant data sets.

So that was on the requestor side. The next two parts are really one big blob at the moment. The group's not defined this, who's got responsibility for this aspect, is that within one party, is that a single entity, is that two entities? We've not got that far at the moment, but just for our thought process, it's easier to separate those out.

So the authorization aspect of that, to do any form of authorization, you need to confirm a lot of the points that the requestor has, so the purpose, the records, the data elements, their identity, and also the legal basis that they're going to be processing the information under. That might be slightly different [to the legal basis that] they're requesting.

Then the third and last part of that is the response. So if everything else has already been confirmed, the response should be fairly easy. There's not many checks to do that. However, the responder has to have its own legal basis for responding to that request. That, again, may be different from the legal bases on the other two aspects. So in theory – probably not in practice – there could be three different legal bases for each one of those aspects. I think we've certainly covered that in some points, but I don't know if we've clearly spelled that out.

Then overarching over all the top of that, we're going to have to think about auditability, transparency and accountability measures across all of those aspects, and that's going to have to be built into the policy about how we maintain that transparency and accountability for that process, and that in itself will allow correct [audibility] as we go forward and allow responsibility to be carried out properly.

Then the small diagram underneath there is just how that all slots in to the overall framework of things, so [set] records, going all the way through, accreditation, and all the accountability measures.

So for us, that was just a good way of thinking about how we're processing the information and the different steps that we're going to have to account for within the policy. Can we go to the next diagram, please?

Like I said, there was a lot of napkins. So this one we've touched on earlier this morning. This comes down to where the responsibility lies for a number of the different aspects. So thinking about the second one, this is where that [inaudible] section is and who holds responsibility for – so what we have here is an assumption that there is an authorizing entity which is separate to – we've put registrar/registry there, but it could also just be contracted parties.

So if you were to put all over the items underneath the authorizing entity, as we have there, they are responsible for the operational – they're operationally responsible for those sections. And as the overlapping part shows, the contracted parties still have an organizational responsibility for those [inaudible].

If that process for [confirming the] purpose and accreditation and everything else is not properly done, they still have responsibility for that. So the policy behind it, their agreement between the authorizing entity and the contracted parties [isn't properly] [inaudible] out, they are responsible and ultimately liable.

So I think that's going back to a slide that we saw earlier from the Strawberry Fields Group or whatever we want to go on that side. I don't think – and this is me personally here a little bit – that you can ever totally get rid of the full liability from the contracted parties side, because you've always got some form of organizational responsibility for the processing that's going on and the providing of the data element is also always going to be with the contracted parties, which they will have operational responsibility for.

At the end of the day, they're the ones with the data that has been disclosed, so they will always have operational responsibility for that. That has to be transported in a secure and reliable method, it has to be accurate, and all the other parts under GDPR. So I think there is no way of getting rid of that operational responsibility from them, and as I've already said, the actual organizational responsibility is also always there, I think.

Before I go on to the actual form, are there any questions about those documents maybe? Is that okay, Janis, to do it that way?

JANIS KARKLINS: Yeah. Let me ask now team if there are any questions or clarification before we get to the next presenter, who is not yet in the room.

And I have Matt Serlin and Ashley in line.

MATT SERLIN: Yeah, thanks. Thanks, Chris, I think this was really useful and a good visual representation here. I just want to echo what Volker actually said in the chat. I think over on the registrar, registry or other responsible party, I think in addition to providing the data elements, there needs to be a bullet in there, or a couple bullets in there to review the request and to make a determination. Those are also operational responsibilities of whatever party that ends up being. And that may ultimately end up to lead to providing the data elements, but I think we'd need to capture the fact that there is an evaluation and a determination as well. Thanks.

JANIS KARKLINS: Thank you, Matt. Ashley, please.

CHRIS LEWIS-EVANS: Can I just quickly respond to that? [inaudible] on that list is exhaustive on the bullets there, and where they fit is definitely a question I think we need to get to. So yeah.

JANIS KARKLINS: Yeah. Thank you. Ashley, please.

ASHLEY HEINEMAN: Yes. Sorry, questioning my own colleague. But I guess my question is – and it kind of builds off of what Matt was asking – is that dependent on what model we ultimately adopt? Like if we can find a situation in which – and get legal assurances that an authorizing entity can be doing the reviewing – because I see it as this: I agree that liability as a whole can't be escaped by the contracted parties. But I think it could be nuanced a bit in that contracted parties have legal liability for the collection of the data, they have legal liability associated with the transfer of the data, but if we can find a model in which looking at this chart here, you have an authorizing entity, that would include the responsibility of reviewing the request, they could take the legal liability for disclosing, and the responsibility associated with reviewing the request.

So that was kind of my question. I originally wanted to propose. I'm not saying that's ultimately what we're going to get, but is that an option that we can be looking at and building policies around? Assuming we'll get to some stage where we get the assurances that the contracted parties would need to feel comfortable with that arrangement.

CHRIS LEWIS-EVANS: Just to quickly respond to that, I think yes, that's possible to get reviewing. I don't think you're ever going to get rid of the disclosing element from the contracted parties unless you move all the data to a central point, away from the contracted parties, which I am not saying that we should do. Just to be clear. Thank you.

JANIS KARKLINS: Okay. Thank you. Any further request, comments? I see no hands up for the moment. Shall we then go to presentation of Georgios?

GEORGIOS TSELENTIS: Sorry, I think the presentation is now for Chris, it's for the – I think it was presented, the flow, so it is Chris'.

JANIS KARKLINS: Yeah. Sorry. Chris, then please continue if you want to walk us through the table.

CHRIS LEWIS-EVANS: Yeah. Perfect. Thank you. So the first thing that we did to change from Thomas' [form] slightly was we added an overarching purpose. [inaudible] going through the previous example on this, I think the user case for that is starting to get broad, starting to become more like a purpose, so being able to link those two to see how they relate and how you might have other user cases underneath that purpose might be helpful going forward, but that's obviously one for the team to discuss whether that’s necessary.

So I'm not going to read it out, because my voice is a little bit monotone and boring sometimes, but that is the purpose that we've identified relating to this user case. And obviously, this is just first reading, so we can always go through that later. And then the user case, which is the investigation of the criminal activity against a victim in the jurisdiction investigating an EU LEA requesting data from a nonlocal data controller. So for example, UK police force requesting data from – I'm now going to pick on Alan a little bit here – an Irish data controller.

So user group is quite simple. If [inaudible] criminal law, national public security, so for us, that’s sort of one group lumped in together, and obviously, there’ll be lots of user cases behind that.

Why do we require this? There's really two aspects that we use this sort of data for. The first is if it belongs to a secondary victim of a crime. So in other words, has that domain been hacked in itself and misused for the crime that’s been committed? Or is it part of the criminal infrastructure involved in the crime, and therefore, are we able to identify further investigatory requirements from that?

So the lawful basis for requesting this, this will be down to local law, so in the case of the UK, if it was myself, I would use the section seven, the [crime courts acts,] which allows us to request data to be disclosed, so that is obviously outside of GDPR, and can be requested.

So that would then go to – going to pick on Alan again, obviously. That would go to Alan, and his reason for disclosing that would be 6.1(f). So Alan cannot work off of 6.1(c) because under the section seven, there is no obligation for him to disclose data. I am also outside of his jurisdiction. Therefore, I'm not considered by him to be a competent authority. So therefore, we come down to a 6.1(f) legal agreement on this. Scroll down a little bit, please.

Lawful basis [processing] data would be the same, it would be under the [crime and courts act] for the [inaudible]. So in this case, it is all down to our due process and local law. In some cases, it might be different. I think they're going to be very rare, but I think it’s worth capturing if we do have a user case.

F and G I'm not going to spend too much time on, because we've gone through safeguards and they're very important, and please [don’t take it I'm disregarding] them at all. The only thing I have done on the form that I think Georgios raised and Mark raised in the last meeting is I got rid of the three sections of safeguards. I think that the data subject rights should be embedded in both the requestor and the disclosing agent, because realistically, what we're trying to do, we're trying to protect the rights of the data subject, and really, the responsible parties are the requestor and the data controller, or the disclosing party. So I think having those embedded in both of those provides a higher level of safeguard rather than just having it separate and not really assigned to anyone.

So I think that assignment of those safeguards is really important, and I think this still needs some more work, I think as discussed in the next one. Scroll down a little bit. Thank you.

So data elements, I know this got shifted up in the other one, but obviously, that was before this one was [created.] Realistically, we require all data fields within the registration data, so [inaudible] RDS.

I think it's a good idea to list all the fields. There's a number of reasons for this, to aid identification and allow investigation. So if we had another source of data with exactly the same information, we were able to match up the two to confirm that it is exactly the same registration.

It also allows us to carry out proper assessment and verification if it is a secondary victim. It's quite important to not treat a secondary victim as a criminal, something that we're very careful for and doing proper assessments and look at any impact. So to enable us to do that, all those fields are required.

And then accreditation, [the user,] is very similar. The last section with few differences with what processing is available to us and how we can use it. Let me scroll down a little bit more if that's possible. Thanks. Up a bit. Is that all of it? Thanks.

So yeah, [tied that down] a little bit. I think some of the things that we've added today – and the other one might need to go in there, but [inaudible] first reading, and this was before we had started the conversation on the other one.

Georgios, have you got anything to add on that?

JANIS KARKLINS: Georgios, will you go now or shall I open the floor for any comments or questions?

GEORGIOS TSELENTIS: I think, apologies, the first slide was the one that I want to make the intervention. The first slide, the one that showed the process. That was the only thing, but I think it was made by Chris.

JANIS KARKLINS: Okay. Then thank you very much. So now we can have a general discussion, if any, and then we will go subsection by subsection, as we did in the previous case. So, any comments of general nature? Milton, please.

MILTON MUELLER: So yes, some general comments. I want to hear more about what you mean by a secondary victim, and I want a better understanding of the mapping of the data elements to your notion of what you need to do with a secondary victim. I just don't understand that at all.

There's some other issues here. it seems like at one point, you cut and paste from the trademark thing, so like in section I, you say you'll only issue disclosure requests with respect to the trademarks where ownership is evidenced. I assume that law enforcement agencies will not be making criminal investigations based on trademark ownership.

And I noticed also missing in your safeguards is the limitation of data elements required o suit the purpose. So I think that really still has to be in there. You may believe that all of the fields are required for your purpose, but you still have to justify that, right?

CHRIS LEWIS-EVANS: Yeah. So last point first, this was obviously before a lot of those discussions, so totally agree with that. That does need to be in there, and that's why I didn't want to spend too much time with it. I think some revision from the discussions today would be good just to properly reflect the discussions we've already had. And yes, sorry, my fault. Copy paste error. My bad.

With regards to the secondary victim, obviously, the primary victim is the victim of the crime, so someone's been attacked, and they are the primary victim so they're the people we are investigating on behalf of. We've identified a domain that's in relation to that crime. We don't know whether the domain holder is part of that criminal group or is a secondary victim, so whether their resources have been used maliciously without their knowledge.

So you're looking a little bit perplexed.

JANIS KARKLINS: So Milton, you're satisfied with answer, but then Stephanie wants to have a clarification question, I understand.

STEPHANIE PERRIN: Thank you very much. I just am having a hard time without a specific hypothetical here. So if a purveyor of goods has been hacked and there's malware there and they're collecting the data of customers, it seems to me the primary victim is the company or the organization, the individual that has the website. The secondary victim – or is it a tertiary victim – are the people who have been purchasing goods from that website; right?

CHRIS LEWIS-EVANS: I'll try to give us a specific example then. Company X has had their data exfiltrated, it's looked like this was deployed from malware which came from XYZ.someothername.net, or com, or any other TLD to not be ...

So at that point, that's where the malware's been deployed from. It's a subdomain off of – has that domain been set up and they're deploying multiple malwares from different subdomains, or did they somehow get access to the system and create the subdomain unknown to the people that are controlling that domain?

STEPHANIE PERRIN: So if I may have a follow-up, when we talk about primary and secondary victims, we're talking about domains. How do you refer to the humans that have the collateral damage from this?

So let me give you an example that would be dear to our hearts as defenders of civil liberties. If you've got free speech advocates operating a website and the data is exfiltrated – is that the correct word? – from that website, including IP addresses, and the families of the folks with the IP addresses are hounded out of existence, are they tertiary victims, or are they something totally separate? Ancillary to the crime, as it were?

CHRIS LEWIS-EVANS: Sorry, Stephanie, I don’t see how this relates to the user case. So what you're saying there is a completely different user case where a site has had its data exfiltrated, the data relates to users of that site or employee [group] –

STEPHANIE PERRIN: Yeah, I'm just trying to nail down our nomenclature here. Primary, tertiary, secondary, and then everybody else. That’s all. Are we considering the impacts? [inaudible] it makes a difference from our perspective. Or are we only considering what falls within the gambit of domain protection? From a risk assessment perspective. Thank you.

CHRIS LEWIS-EVANS: Sorry, I –

STEPHANIE PERRIN: Forget it, I'll write it out and pester you later. Thanks.

CHRIS LEWIS-EVANS: Yeah.

JANIS KARKLINS: Yeah, probably makes sense to both of you get together and try to clarify terminology. Amr is next on the list.

AMR ELSADR: Thanks, Janis. [Chris,] you mentioned earlier that it made sense to you in this use case to embed the safeguards for the data subject in the other safeguards, could you point out where that is? And also, explain why you reached this conclusion. And considering that the data subject might actually be the subject of the investigation, is there not a conflict here where the – see where I'm going with this?

CHRIS LEWIS-EVANS: Sort of, that makes sense. As I said, I think it‘s the right thing to do, because it’s putting the who is responsible for the different rights. I've literally put one line – sorry for going to – I think it’s in G or H – and this is [inaudible]. So G, yeah. Thank you.

So [inaudible] in compliance with data protection laws such as GDPR, including secure transmission and data subject rights. I think [they’ll need to be better listed.] This was before we’d broken those out.

But for me, it makes sense that we assign who is responsible for carrying out those safeguards. Do we call them safeguards? Do we put them into terms of service, user agreements? Barrier to entry that you are going to carry out your process in compliance with this? How we do that, we've not got right and I don't really want to get too [inaudible] because I think it is very important that we get that right and that we mention code of conduct and everything else. I don't think we're far enough through this process to nail it down to exactly how that's going to be laid out. But I think it's just at the moment it's a little bit messy and we're lumping lots of problems into one bucket and I think we need to make sure we assign the responsibilities and then how they're carried out in a proper process. Does that answer your question?

UNIDENTIFIED MALE: Yeah. Thanks. It answers one of them but not the second. A potential conflict of interest here because if you're embedding the data subjects right under the requestor's safeguards but the requestor might actually be investigating the data subject for potential criminal activity. So, is the requestor the right party responsible for safeguarding the data subjects rights in this case?

UNIDENTIFIED MALE: So, it depends on the rights, and obviously everything we do we have to look at and assess the inter-proportionality of what we're doing, so that is embedded in some of the rights and we're obviously tied down by the human rights laws and everything else. We have to take all of that into consideration when we're processing it.

As we move forward into other user cases, then yeah, I can see that becoming maybe a little bit more of an issue. I think with other user cases, certainly, but there's lots of protection within law enforcement agencies processing of personal data and data belonging to subjects under investigation that we put into process.

So, in this case, I think we're probably okay, but I can see in other user cases, we might need to think how we put that down properly. So, I've not thought about it in great detail. Like I say, these sections need a lot more work I think, and I think realistically – and it might be a question for the chair – is whether we want to have a small group working out how the safeguards are aligned, whether we want to call them barriers to entry or user agreements and how we do that I think is quite a big piece of work and a very important piece of work.

JANIS KARKLINS: Thank you. I have next Hadia.

HADIA ELMINIAWI: So, this is just a quick comment. With regard to [inaudible] question and the conflict that sometimes might occur in relation to the data subject, there are actually articles in the regulation that speak about that and you can pull them up. I think the law already regulates this part that you were talking about in relation to law enforcement agencies. You just need to look them up but there exists articles that speak to this point.

JANIS KARKLINS: Thank you. Chris, any reaction?

CHRIS LEWIS-EVANS: No.

JANIS KARKLINS: That was just a comment. I do not have any further requests, so let me ask a question. Can we scroll up on the very top of the screen?

Whether that would be useful to think in terms of overarching purposes for the cases, in general, whether that would provide any added value for our conversation.

UNIDENTIFIED MALE: Can you repeat that question?

JANIS KARKLINS: In this case, we have overarching purpose. The question is whether it has any value for our exercise and whether each case that we're examining should have overarching purpose as a statement at the beginning. That's the question, what that would give us in terms of policy recommendations that we're trying to extract from this exercise. Nothing?

MILTON MUELLER: Yeah. That is a question that was kind of in my mind, too. The overarching purpose is extremely broad and could be broken down into five or six different use cases, if you wanted to. Then, in the case … I think we're getting more into what we need to be doing when you get into the specific use cases listed here. Criminal activity against a victim in the jurisdiction and outside of the jurisdiction. Those are much more specific in terms of where we are right now.

Obviously, everybody knows that governments have those overarching purposes, but how helpful those are in this particular context, it's not clear to me.

JANIS KARKLINS: Thank you. Georgios?

GEORGIOS TSELENTIS: Yes. I just want to highlight that, as you saw in this use case, we made a specific – we narrowed it down to where the requestor is in a certain jurisdiction and the data controller is driven to another jurisdiction. Initially, we had all possible combinations and we saw that this is getting extremely out of proportion because this has an impact also on a legal basis that are used in the possible scenarios that we have.

That's why you see probably that we did the opposite on what just Milton said on the overarching purpose. We try at least there to get a grouping of things that we thought could stay consistent under this scenario.

We can split that to as many use cases you might imagine. The important thing is to see that how this splitting then affects later on the other decision, in particular the legal basis that we are doing the processing activity.

JANIS KARKLINS: Thank you. Margie is next in line. Margie?

MARGIE MILAM: I think the overarching purpose is useful here. It helps explain what you're trying to get at. And I think we probably need something like that as we build out the templates anyway for the other ones. Thank you.

JANIS KARKLINS: Thank you. I don't know if you have any further requests. My suggestion would be the following. Probably taking also into account time at our disposal, it would not make sense to go in detail reading of this case at this moment, but rather to switch gears and try to identify what other cases we would be having. I note that there have been already some volunteers who said that they would attempt to write cases also for our examination. I will now try to refresh my memory. I think that IP folks will write a few cases, apart from the one we already examined.

So, I understand that SSAC will attempt to write a few cases – three cases – on mainstream issues that they are dealing with. I understand that business community wanted to write at least one case, right? Who else?

The reason why I'm asking this is to understand what would be scale of our exercise in getting through those cases. So, for the moment – and then law enforcement. I think you were talking about a few additional cases, right, Chris, or this will be the only one that we'll be fine-tuning and we'll be working on?

CHRIS LEWIS-EVANS: Yes. There was actually a second one which was just a slightly different jurisdictional basis.

JANIS KARKLINS: But that's important. That is still considered as a second case, then. So, you will have two cases.

CHRIS LEWIS-EVANS: That was attached to that and then it's up to the group whether you wanted another one that was non-criminal. Whether that's regulatory or civil, we can have a look at that as well.

JANIS KARKLINS: Please, Alan?

ALAN WOODS: Just when it comes to the use cases, I think the value in these use cases specifically will come where we will both see the similarities between certain use cases where, say, in a 61F you find that the same repeated steps are being across the board. I think that will be very helpful for us to understand where we're all coming at it from angles, but ultimately, it might end up at the same sort of process. But also I think, especially as Chris has just pointed out with his use case is that there are specific changes in the way we must approach certain ones and I think it's very good for us to be able to highlight those specific changes that needs a different approach, say, by whoever the SSAD or whomever.

I just want to caution that I don't think we need to start creating a catalog of copper plate templates. What we're looking for is, again, these indications of the unities in the processes and the way we can probably streamline the processes going forward. It's not just we all try and get our speak in at this particular moment in time. It's so that we can help forward in the understanding of everybody in this process.

JANIS KARKLINS: No, actually, probably we need those looks in different mainstream cases in order to understand the implications also for the sake of the process. Therefore, it is important that, for instance, if we look on security aspects. So, we examine three mainstream cases. One probably on … Now I'm speaking on top of my head, but you may help what you're thinking in terms of what would be those situations that you would try to describe.

BEN BUTLER: In consultation with the rest of SSAC we were thinking obviously there' a myriad number of cases that are security or abuse related that we could go through but we think that there are three larger, overarching with key differences.

One would be a security research type situation where all they're looking to do is be able to correlate data. So, pseudonymous information might be acceptable. But that's completely different than, say, operational security where they need to be able to contact whoever owns the other website or network that's attacking them. And then a third one would be reputation service providers who are kind of sitting outside the direct communications back and forth between networks.

So, we think those three can get us real close, as far as focus on security, if there is an appetite for this group to go through those. We can pare it down if that's more preferred or expand if it's preferred.

JANIS KARKLINS: I think what would be important is to write those cases which would represent, let's say, mainstream majority real-life situations that we could assess and design the system based on mainstream cases rather than marginal cases. In marginal cases, there always will be probably specific measures taken in order to address them. Thank you, Ben. Margie, your hand is up. Your hand is not up. It's already down. Marika, your hand is up.

MARIKA KONINGS: Thanks, Janis. One thing we flagged when we started going through the updated use case on the IP cases, staff has already started to think a little bit ahead as well about the other topics that are included in the SSAD worksheet. From our perspective, there are a number of those that are also specific to use cases.

So, what we've done is expanded the template and, if people agree, we'll post a clean version of that on the Wiki page, so hopefully those working on the use cases can use this updated template and hopefully maybe we can see if Thomas is willing to expand his original use case as well with those additional data fields, because the idea is if we are able to gather than all together now, it will save us time down the road because we will need to look back at those additional questions.

So, just to give you an idea – and it goes a bit more to what type of information is required to be provided for or requested is made as part of that use case, what is the expected timing of a substantive response when a request is submitted following the use case? Is automation of substantive response possible, desirable, in that specific use case?

I think a question that came up before as well, how long can the requestor retain the data disclosed and what are the requirements for [destruction] following the end of the retention period?

So, those are some of the additional categories we would suggest adding to the template with the hope that that information can also be provided so we really have a very complete set of information in relation to each use case, as again, those are also topics that were already identified in the SSAD worksheet. So, the hope is by adding it here, we're actually saving ourselves time by not having to go back to that at a later stage, and then for each case, still look at those questions as well.

JANIS KARKLINS: Thank you. If I may suggest that staff will send out the master template for all those who are writing cases, that you can use more or less the same template at the beginning, and of course please feel free to modify that template as you deem appropriate for your case. But at least all the required elements that we think would be useful to have based on our work plan program and charter, we would have them already in that template and we can go through them together. Alan Woods?

ALAN WOODS: Thank you. One thing that Marika said about the addition of the data retention period. I personally think – and, please, I could be just not correct on this. I think that's probably not necessary, because you must remember, that when we disclose the data, that data goes into the controllership in a separate processing situation. So it's up to that person to set their own limits and retention period. It's not really appropriate for us to say to them, "You must retain for only X amount of time." It's up to them, at the end of the day, to deal with that data. So, I think it might overly complicate it, unless there's another instance in which people think that might occur.

JANIS KARKLINS: Thank you. Berry?

BERRY COBB: Thank you, Alan. I think the original intent, because it was one of the topics that we had listed a long time ago and I think the original intent was more about once the data was used for that particular purpose, how would it be destroyed? What are the policy questions about getting rid of it once you've used it?

ALAN WOODS: Agreed, and I think we talked about it briefly yesterday about that – I think it was [Kristine's] idea about this whole concept of can you inform us when you have used it for the purpose I think more as a safeguard. In that sense, it makes sense. But again, I think we're probably stepping on ant hill we don't need to near on that one.

JANIS KARKLINS: Thank you. I think a negative answer also is an answer for the purpose of the policy development, so therefore I don't think we need to shy away to ask questions that potentially may have implications, and if turns out that they're not needed, we will drop them. There's no issue with that. Marika?

MARIKA KONINGS: I just wanted to confirm as well. So, are the both aspects you think are not appropriate for the templates or the retention period as well as requirements for destruction following the end of the retention period and not for … They're not for here, basically?

ALAN WOODS: Knowing … And it's my opinion as opposed to somebody … Yeah, I think potentially we can save ourselves a lot of heartache. But as Janis was saying there, it might be good leaving them in and having the negative answer that … It might be beneficial. Apologies if I've interjected wrongly.

JANIS KARKLINS: Thank you. My next question is would authors or penholders of those cases, would they submit those cases by end of next week? Not tomorrow but seven days after tomorrow. So, can we then take note of this action item, that that would be a deadline for submission of all cases based on templates that staff will be providing. And to my count, we have nine cases for the moment and I would not be surprised that we would get additional one or two as we go. So, I do not expect having more than a dozen, twelve, but as we go we may have some additional ideas that would be needed.

So, if that is the case, then we will have by end of next week. Next week all of us will have deserved one big break. We will not have meetings of any kind next week. So, we will have them considerable work to go through in order to examine all those cases one by one, and as we see, probably one meeting will not be enough to go through each case. So I would say maybe two meetings, and even then some of you may think that I am optimist – I am, by nature – which means that we will need many meetings to go through and we do not have that much time on our hands. So, the question is what would be the method how to go through and do this work.

Also, keeping in mind that there was a very clear request and my promise that there would not be more than two meetings per week per each team member. Ideally, one meeting per week. But certainly not more than two.

So, when you put all these things together, clear math says we would need probably six months to go through those twelve cases. Impossible. So, therefore, only way how to do it is to delegate – to delegate responsibility to sub-teams. My suggestion is to think in terms of maybe even three sub-teams of the team and each sub-team would go through three cases in the time period July, mid-August. That's more or less assumption that we could do. Which then would allow us to, let's say, do the write-up and finetuning of all those cases, as well as the initial attempt of synthesis, of whatever trends staff will be able to see in all those finetuning written-up cases. And then provide the synthesis material at the very end of August or very early September. That would be material that we would work on during next face-to-face meeting in Los Angeles in mid-September.

So, that is my proposal. I would like to open the floor for any reactions you may want to have. I would seek your non-objection. Otherwise, we will not be able to demonstrate the progress – substantive progress – as it is requested from the team by November meeting.

Once again, proposal is to constitute representative three sub-teams. These representative sub-teams would examine each three to four cases in the period of mid-July, mid-August and then we would have material either late August, early September to work on during the face-to-face meeting, including with the moderators and facilitators of conversation. So, that's proposal. I have a few hands up. We'll ask Marika to put hand down. That's a new hand? Then you have the floor.

MARIKA KONINGS: Thanks, Janis. As people think about your proposal, I'd also like to suggest, because we do have as well under the next item, your various prepared project plan and it would also be helpful to maybe consider it in conjunction the conversation of meetings going forward and intensity.

But one thing I did want to flag as well in relation to additional use cases, I just wanted to as well encourage everyone to maybe have a look at where we originally started, the list of purposes, and really make sure because I think most groups are now preparing use cases from their specific group's perspective, just to make sure that we don't forget about a group that may be in there. I'm thinking, for example, the general research category. I think we had one there. And maybe people think it's not necessary to have a use case on that but just to make sure that, if there are additional ones, that ideally we identify them as soon as possible and find a volunteer to take care of those as well.

JANIS KARKLINS: So, let me then take a few reactions that I have now here. Then Berry will walk us through his prepared time chart and presentation. But let me see first reactions. Alan Greenberg?

ALAN GREENBERG: Thank you. I'll point out that if we form three sub-teams, those of us who only have two members on this group are either going to have to walk away and not participate at all in some of the sub-teams or one of the members is going to have to take a double load and I think that's not reasonable. Thank you.

JANIS KARKLINS: Can't we think of involving alternates as a supporting staff specifically for that case?

ALAN GREENBERG: We could think about it. In the past, when that's been mentioned, it's been vetoed.

JANIS KARKLINS: I have no baggage of the past. I am new in town. That's [inaudible]. Thank you, Alan. Amr?

AMR ELSADR: Thanks, Janis. I've expressed concern about the pace at which we were moving previously, so I won't repeat that. I realize that within the same timeframe we're going to try to complete this work. We're also going to be bringing the priority to the topics to the full EPDP team. So we're going to be working on all of these things together. And if we're targeting the next couple of months to work through these issues, I'm also wondering if some of us might have – we're going to be taking time off during the summer, possibly. Not too long, hopefully, but some time off. So, I just wanted to flag that as an area of concern as well, but I'm not objecting, to be clear, to trying to work through this timeline. But figured it's at least note-worthy to mention. Thank you.

JANIS KARKLINS: I understand that, and again, I think we should honor our own commitments. My commitment was not more than two meetings per week. I really want to commit myself to handle that, but from other side, we also need to deliver. Hence, I am suggesting that we should start delegating without hesitation because, ultimately, we will review all those cases as a theme anyway and delegation is a normal practice. I think that every businessperson would confirm that delegation is the only way how you can really survive in that intensity of business activities that you have. And usually if those people who do not delegate, either they fail or they get burnout.

Therefore, please think in terms of delegation without hesitation. Trust your team members who would be examining part of the cases. You will be examining part of the cases and then all that will come together in one synthesis or attempted synthesis document that we will look through together. But your concern is noted and this is permanently on my mind. Chris Lewis-Evans, please.

CHRIS LEWIS-EVANS: Just one point I think that's been raised from the two use cases we looked at today. I think Mark might maybe have the same sort of point is we've highlighted that's an area that's common to both already. There's a lot of overlapping work on that. There's also, I feel that we've also agreed that there's a lot of work that needs to be done to that to make that look right. If we're splitting into three separate teams straight away, that's work all those three separate teams are going to have to do separately which is repetition. So, I think we need to sort that out first before we then go and split into those three teams. I think there's definite need for that to be complete first and that will save a lot of work. And I think for a lot of the groups that will be a lot of copy-and-paste and hopefully better than I can do it.

JANIS KARKLINS: Thank you. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I don't specifically object to the approach you laid out. I just think we need to make sure all of us are clear and on the same page as to what the goal is in creating all these use cases.

I don't view the use cases themselves as the end result or the end goal. The use cases, as long as they're just a tool in helping us develop our policy recommendations, then I see this as a valuable exercise to help inform our work in developing those policy recommendations. But trying to identify all possible use cases, use cases that may change over time, I think that's an exercise in futility. So, I want to make sure we don't get wrapped the axle spending too much time on use cases themselves, but rather keep in mind that they're really just a tool to help us develop the policy recommendations. So, I wanted to get that point out, but that said, I don't have objections or heartburn over the path you've laid out.

JANIS KARKLINS: Use case is a tool to get better understanding of touch points that we may have, all of us. Then, out of those eight, nine cases we have, we would extract trends that we would probably constitute the beginning of our policy document discussion. The aim is to have that initial policy document ready for September meeting because it would be much easier to do the first reading and the first [threshing] of the document when we're seeing each other that we can also use different methods of group work when we are in the same room. That's why we're a little bit rushed. I understand that. Hence, my proposal to split tasks and then to have this conversation in three separate groups. I commit myself to be on all of them, so it would be a really big hurdle for me, and for staff, that will do also additional work for that. But this is the only way how I see we can try to keep up with our expectations from us by others.

CHRIS LEWIS-EVANS: Can I just respond?

JANIS KARKLINS: Yeah.

CHRIS LEWIS-EVANS: That sounds great and thank you for that. That sounds good for me. I guess a quick question for Alan. Hearing what Janis just said, would that make you feel better that maybe you didn't have to attend each of the subgroup sessions with that in mind?

ALAN GREENBERG: No, probably not. Remember, we're dealing with team sizes, including alternates, that range from three people to nine people here. It's a very significant difference in load, especially given that it's summer for many of us and some people may actually want to take a bit of vacation. At-Large has four. The Business Constituency only have three, including alternates. So, it's a real difference in load.

JANIS KARKLINS: I appreciate that. But again, point being this is not the end of the story ALAC's perspective is extremely valuable and needed in all this conversation, but if you will be missing one out of three discussions, it's not the end of the world. I understand your desire to be on all three present. No objection. Maybe we could think of alternates who could join in and then provide perspective from your group's side. I see no reason why not doing, exceptionally in these circumstances when we have those additional groups formed.

But let's hear further comments. Next is Matt, followed by Volker.

MATT SERLIN: Thanks, Janis. I just want to echo what Mark said. I do think this gives us a really good framework with which to work. I think the timelines are reasonable. I'm sensitive, Alan, to your point as well. I guess I would ask for as much flexibility as we can within the small groups. So, for the registrars, there's six of us, plus Zoe who is really the important one. But based on people's availability and comings and goings to the extent that we can slide people in and out as needed, I think that will be really important. Also, I'd ask that we allow for observers to participate in the sub-team calls as well. But I think it's a good path. Thank you.

JANIS KARKLINS: Look, I think everything is possible if we want to do things. I think that when I say subgroup, I do not really mean fixed subgroup which could not be changed in any way. I would say we could call them one, two, and three just to be different from ICANN Org. Then if one member wants to be one week in call for group one and the second week in call for group three, fine.

Ultimately, all these calls will be open anyway for anyone who wants to listen. So, the most important thing is that we have substantive conversation where we could capture all perspectives and try to nail down these commonalities for preparation of the first policy draft that we're aiming at. I see Volker. Volker, please.

VOLKER GREIMANN: One point I would like to make is something that we discussed in the beginning when we were talking about these timelines, which really—

JANIS KARKLINS: Sorry, Volker. Could you speak slightly louder that we can hear you?

VOLKER GREIMANN: Sorry, I didn't realize. One point that we made originally when we agreed to these timelines was that these were completely arbitrary and that there was no obligations to meet any of the deadlines that we have set to ourselves but they were rather aspirational. I don't see that there is an urgent need to meet them at this stage and splitting us up into subgroups that would make binding decisions I think is a bit problematic for the reasons that Alan described, and also for the amount of work that has to happen aside from making those groups possible because there will have to be coordination and reporting and discussion amongst the members of the group that cannot be there but would still provide input. So, the background work would probably triple as well, so that's something that needs to be taken into account as well. Basically, let's not rush this. Let's do this right and let's make sure that the process that we employ is properly set up that all groups are properly represented and no one is subjected to burnout.

JANIS KARKLINS: Volker, one thing that I want to push back. The outcome of the work of these groups by no means is binding to anyone. This is just material, a method how to get to the commonalities of different issues that we are talking about. And the team will be examining those commonalities as a team and [inaudible] come to the conclusion, so then they would become, let's say, the outcome of the activity.

The timeline is not really arbitrary. This is dictated by outside possible threats, if I may call them threats. We heard very clearly that if we will not deliver or demonstrate substantive progress by end of the year, some legislators will make decisions for us and then we will be following their decisions rather than providing our own opinion on these very complex, difficult issues.

Hence, there is urgency in this exercise, at least to demonstrate substantive progress. Therefore, I would beg your support in understanding these outside emergencies or pressures that we exercise. Alan Greenberg is next.

ALAN GREENBERG: Thank you. I originally put my hand up for the item that Mark mentioned. That is when we started this discussion I and others said these have to be some examples to guide us, not a thorough review of all possible subjects or samples and I still have a level of un-comfort with the number that we're now talking about. So, I guess I'd like a little bit of clarity on that.

The other item is you've mentioned a number of times that we could use alternates for these groups. I haven't heard any objection, but on the other hand, it would be nice to have confirmation from every group around this table that they're not going to object to that if we're going to go ahead with that plan.

JANIS KARKLINS: Thank you, Alan. I think everyone heard you, and if somebody will object, they will spell it out very clearly. Ashley, please.

ASHLEY HEINEMAN: Thank you. Ashley with the GAC. I'm saying this at the risk of really upsetting all the people who work really hard already but I think we're at a point now where we might even be giving us too much time for this exercise because I think we've gone over a hurdle of understanding what the format is. Chris was able to crank this thing out pretty quickly. I think we kind of know what's expected of us. It also, I think, puts into perspective that we don't necessarily need a whole lot of case studies.

So, I would urge us all to try and achieve this, because once again, this is a tool. We need to get to the actual policy development and I think this will provide the framework that's probably necessary to keep us chugging along at the appropriate pace.

JANIS KARKLINS: Thank you, Ashley. Alan Woods?

ALAN WOODS: Thank you. I am not going to say again what Chris and Mark both said but they stole my thunder somewhat. But what I will just add is that the whole point in my mind of these case studies was so that we could collectively come to the same conclusion and learn from the experience of going through these case studies, and again if we're coming out to these realizations in three separate groups, yes, I know we expect to go back and discuss it with our groups but it will cause imbalance between understandings and that to me will just lead to misunderstandings going forward. So I would caution against going outside of the learning experience which this could provide for us.

JANIS KARKLINS: Thank you. Georgios?

GEORGIOS TSELENTIS: Yes. Similarly, I wanted to ask you, Janis, maybe it's better that we devote more time about how we are going to fusion those results. I think, as I said, we have several use cases. We can go very deeply and analyze them. I think the value, as some of the colleagues said, is how we are to have a very good plan how to fuse those. So, what's in the timeline for this?

JANIS KARKLINS: I think I mentioned timeline. First of all, I have witnessed many times when collective drafting is failing. So, I do not intend to start from white sheet of paper in the group of 30. I think it would be a task of the staff who would be present and holding pen on every discussion we have about cases to distill commonalities and put those commonalities on paper and present that paper for the group as a first draft which probably will be killed and redrafted by us. But at least we will have a basis for the conversation and that basis will be prepared by staff. This is how it's a classical scheme how it works. European Parliament also gets the documents from the staff, from assistance. So they work and then deputies are looking at those.

I would aim at getting that document prior our meeting in September, but in order to get enough material to do the synthesis, we need to go through the pain of examining cases to thresh out those issues.

If we are fine in doing three cases or four cases as a team, okay, let's try. I would see more we go through similar cases, it would be like with the foreign languages. If you learn one, then it's much easier to learn the second. And if you know two, then you can learn third and fourth in no time. So, more cases we will go through, more commonalities will bubble up in a natural way and that will give staff security to put those commonalities on paper and present them to us in one way or another. So, that's my thinking and my proposal.

If we do not – and I feel that there is no agreement on splitting in three – maybe we can think of splitting in two. I'm happy to meet every day because I like the company. If you do not want to meet every day with me, then meet every second. Let's split our efforts and then do this work that we can produce some result.

And I understand the pain, believe me, but we need to deliver. Otherwise, somebody else will deliver for us, maybe in a different way than we would wish to. Hence, my appeal to you. Please, consider my proposal in a positive light. Stephanie?

STEPHANIE PERRIN: Thanks very much. As you might have gathered, I'm all about risk assessment. I'd like to know who's going to deliver for us. I will tell you right now that I am at the edge of burnout and ready to resign because I don't like to not fulfill my responsibilities on this group and I think I come with a fair background, so it shouldn't be so crippling to keep up. But it is. I'm very behind. So, I'd like to know what the risks are of slowing down. Who is going to deliver a solution and how do we know this?

JANIS KARKLINS: Ashley, would you repeat the statement of your government? Sorry that I'm pointing to you but I think it's appropriate this time.

ASHLEY HEINEMAN: Sure. Yes. Our [inaudible] secretary, the head of NTIA, has sent a letter to ICANN basically articulating that if we do not see considerable progress by November, we will be exploring alternatives, including domestic legislation.

JANIS KARKLINS: I'm not sure that we will be able to influence domestic legislation in the United States. Stephanie?

STEPHANIE PERRIN: I don't wish to challenge that statement by any means, of course. I'm sure it's a true statement. But we already have trade agreements with clauses that require this. Most of us who are in trade agreements are already living with that reality.

I don't see that that is a reason to destroy the fabric of a multi-stakeholder process by causing some of us to drop out. Thanks. That's all I'll say on that. Thanks

JANIS KARKLINS: Thank you. Milton?

MILTON MUELLER: On a more constructive note, I would like to just say I don't think this is a big problem. I think there's one or two other case studies that I may have time to just throw one out there the way Chris did. Whether you deal with that through breakout groups or not is, to my mind, purely a matter of efficiency.

I really think … I can't see us doing more than four of these before we really get the knack of it. I think one of them has to deal with researcher cybersecurity and that's one I'm going to try to take a crack at, obviously to liaise with the SSAC people as much as I can. I'm not sure what other ones are necessary unless you break down the law enforcement one into different pieces. Maybe I'm forgetting something. But really, we can do this. We can come up with one more of these. It won't take as long as the trademark one did because that was the first one. So, let's not obsess over this.

JANIS KARKLINS: Okay. Marika?

MARIKA KONINGS: Thanks, Janis. I heard someone I think mention, or suggesting, to have observers participate, but I just want to point out that we currently have 190 observers on our list so that may create a bit of a [inaudible] dimension.

I also know Janis just said that all meetings will be audiocast, but I think it's something we need to look at logistically because usually smaller teams run under a different kind of phone bridge, so we would need to see if that is possible, especially if we're running meetings in parallel. Of course, all meetings will be recorded, and I think with the new Zoom facility, there's as well a pretty decent transcript that comes out immediately. It's definitely not a question that it will not be made available, but we just need to look into the practicalities of doing that real-time.

JANIS KARKLINS: Okay, thank you. Then let me try from different side. Would anyone object the intent of presenting what could constitute the initial draft of policy recommendations for our face-to-face meeting in September? Would everyone object that, let's say, objective. I would say that this is too early for us to do.

UNIDENTIFIED MALE: Sorry. Can you repeat that again?

JANIS KARKLINS: I mentioned that my idea was that the first draft of policy recommendations, or let's put it zero draft of policy recommendations, would be presented in late August, early

September by staff as a result of our discussions of case studies. Marika?

MARIKA KONINGS: I just want to note that of course staff can only do that based on the work you do.

JANIS KARKLINS: Yeah. That's what I'm saying. Based on work we do. Is there any objection for that [inaudible]? No? Okay.

So, then we have two options. Either we provide a lot of material for staff to work on by working ourselves intensively, as I suggested in parallel groups, or we can limit number of cases that we go through, as Milton suggested. One case of security, one case law enforcement, one case intellectual property and we have already basically gone through one case and slightly broadened the scope of it. Then staff will try to extract whatever commonality comes out from examining those three cases. So, then we would continue working in one stream as a team examining those cases one by one in the plenary [inaudible].

But the consequence is, then, staff will have less material to analyze and propose as commonalities. So, if group is fine with that, we can pursue also that and prevent from, let's say, unbearable pace of activities. So, any reaction? Casual walking through the summer with three cases. Ben?

BEN BUTLER: Well, as far as a reaction, the benefit that we're hoping to derive from going through these use cases is to be able to see commonalities and patterns that will help craft the policy recommendations. Statistically speaking, if we do eight or nine, the chance of finding a pattern is far better than if we do three or four. I think if we're really going to give it our best shot, we should do the eight or nine – I'm not advocating for 30 or anything like that – but I think, like Milton said, the speed with which we go through these is going to increase as we do more. So, I think we should do more.

JANIS KARKLINS: Thank you. Milton, are you in line? No, you're not in line. Okay. Let's then do it this way. Aim is to produce the zero draft of policy recommendations end of August, beginning of September. Cases will be written by volunteers by end of next week. Probably they should be written as a one case but maybe with modifications which may give you different aspects of specificities of the case and we will examine those cases in plenary mode every Thursday starting from after next week, whatever the date is – 11. So, would that be acceptable? Okay, thank you. You want to say something?

ALAN WOODS: Thomas Rickert is on a flight at the moment unable to speak and he did put something into the chatroom, so I just wanted to make sure that he gets on the record. He just says, “Hi, all. In terms of using our resources wisely, it doesn’t make sense to work on all use cases now. Or would it be good to really work on a greater level of granularity, the required policy based on one or two examples, and then try to get feedback from the European Data Protection Board?” I just wanted to put it on the record so that people may want to have comments on that and doing that for him.

JANIS KARKLINS: Thank you. It is noted. With this, we have then agreement on way forward until September meeting, and then at the end of September meeting, we will talk about next steps. I think that would be the wisest way of doing because we are faced with a lot of uncertainty. So, hopefully, we will be able to distill all the commonalities out of those cases we will examine.

With this, I think we now are ready to go through a presentation of Berry on the timeline and the resources. Berry, you know better than I do what is in the presentation. Or you should know better than I do. Please, the floor is yours.

ALAN GREENBERG: Janis, if I could interrupt.

JANIS KARKLINS: Yes, please, Alan.

ALAN GREENBERG: I have two leave in about two minutes. Will we have clarity on when we'll have invitations for the September meeting, so we can plan for that?

JANIS KARKLINS: Your question will be answered immediately.

ALAN GREENBERG: Thank you.

MARIKA KONINGS: Thanks, Alan. We're actually working on the notice email, so expect that to go out hopefully, by the latest, early next week.

JANIS KARKLINS: With this, Berry.

BERRY COBB: Okay. So, now it's project management wet blanket time. I guess it may have been helpful to try to go through some of this prior to this discussion. First thing, I sent these around last night. I doubt you've had enough time to really absorb them. There's still very much work in progress. Nothing is written in stone here. But I think an initial takeaway of the work products that we're about to review through is very similar to what we did in phase one about starting at the top and drilling down. You may remember that funny slide about drilling for data elements and starting at the ground and getting way down into the [inaudible]. Same concept applies here. The summary timeline and the subsequent work products, they get more miniscule or get to the micro-layers we drill down.

So, the first slide or the first page here is a summary timeline. The dates or the rough dates that are listed here match what was included in a presentation I think at about middle of May but we wanted to get something that was a little bit more familiar with what we used in Phase 1 so that we can constantly communicate our progress. So, there's really not a whole lot different here.

The one thing that I'll note that doesn't exist on any of these work products – well, first and foremost is the number zero which is the priority coordination with the strawberry group. That is in our scope but it's not necessarily a part of the EPDP charter, per se.

But it will consume our resources and attention, so we will be tracking that.

But then, also, keep in mind what's not on here. More specifically, we've got the EPDP IRT going on for Phase 1. That is also time-consuming as well as some of the other smaller items that we have, like the legal committee and those kinds of things. Next page, please.

So, page two here is kind of a new development. For those that are familiar within the GNSO, they're working on PDP 3.0 and there's a series of recommendations that were created from the strategic planning session about how to more effectively manage the working groups that the GNSO has active now. One component of that is attempts to understand the status and condition of our projects and being able to identify up front or early on when we're about to get into trouble.

The point of this, first and foremost, in Phase 1 we had to do weekly status reports to the council. At this point, that requirement doesn't exist, but at the very least, it will occur at the council meetings on a monthly basis. But the most important part of this particular work product is more or less on the right-hand side. The lower right quadrant is more or less set up to talk about what we've done, what we're doing, and what we're about to do as well as list any issues or risk that we may encounter.

What's important, though, the status and condition components. As we drill down into more of the dates that we're going to be setting for ourselves, should the status or condition flip to yellow, more likely it's going to be status which is [mostly] around the schedule of what we are planning to do. If that flips yellow, we're basically obligated to go to the GNSO Council and explain why. So, this does tie in to how aggressive or not aggressive the group wishes to work and it definitely applies to, once we set a date and we start missing those dates, that trickles up hill to affect the overall project plan. Page three, please.

So, unfortunately, I wasn't able to get a full-blown project plan built yet. I only included this as a placeholder but this is what is being built. 99% of the people in this room probably very much dislike Gantt charts. I love them in the fact that once you establish task and the dependencies and the duration, if you miss one date at the top it trickles down and effects the entire plan of itself, and most importantly, the critical path.

As an example, I guess why I'm glad I don't have it ready to show you yet is, if I did, I'd already be changing it based on today's discussions. I think one thing that's very important for this group to understand is to not necessarily fall into the trap – although the summary timeline does do this – is not to fall into a trap of looking at this at a calendar basis. Us going through this first topic exercise of defining … It started off as defining common user groups has now evolved into use cases and the like.

Had I had this project plan built before we started any of this, we would be in yellow condition and already be talking to the GNSO Council about it.

So, when I do build this out and we get agreement about the tasks that are going to be laid down and the durations associated with them, they're going to be with the concept of the amount of hours it takes for this group to deliberate and come to agreements on particular topics. I think it's one of the main issues within the GNSO that again we fall in this trap of thinking we've got a year to do this. Well, in a year's time and 1.5 hours per call, you only really get 100 hours of actual deliberation whether it's via audio or in face-to-face.

I to have this next version next week for initial review, but ultimately, this is the foundation by which is the approval of the work plan that we're seeking that we do need to get approval not only amongst ourselves but with the GNSO Council and having this is contingent on this group getting any more resources from the board. We were fortunate that we were able to get the resources for the upcoming face-to-face meetings but noting that there's such a long lead time to do that. For example, that includes funding for the legal advice, etc. Page four, please.

This is where we drill down into the nitty-gritty. I think in the past you've seen different kinds of work plans that were in table form, but typically included 20-plus or so rows, if not more, and they went out three or four months in duration. There's going to be several of these floating around but these will be in Google Docs and we're all going to be empowered to help manage these.

But once we identify either a task or an action item, we're going to assign who it's assigned to, when it was assigned, when it was due and whether it's complete or not. I'll defer to Janis as to what are the consequences when we miss a date, but just from a project management perspective, if we miss a date here at the micro level, as I mentioned earlier, it trickles up top. And if we miss enough of these, then it flips our condition to yellow and we get in trouble with the council. So, that's the intent of that. You can go ahead and move to the last page.

The next page is just the action items that we'll start filling out. There's a whole bunch of them coming out of this meeting.

Then, the last page is the fact sheet. This should be familiar to you as well. We've created a new one for Phase 2. It is loaded with some of the resources that the board recently granted to us for the face-to-face meetings. The fact sheet is purely a communication tool, although it does include some high-level milestone completions and some of the other aspects.

The numbers you're seeing in the financial resources here are what we had requested prior to this meeting, most of which wasn't used, except for the few that asked for funding to come here to Marrakech. Once we flip over into the next fiscal year, then you'll see the amounts that the board just adopted for us.

But, as I said, outside of the resources that we have that we just got from the board, we don't get any more until we have a true, fully approved work plan and project plan by the GNSO Council.

I think that's all I have for now. Stay tuned for more. Thanks.

JANIS KARKLINS: Thank you, Berry. Any questions to Berry? Marc Anderson?

MARC ANDERSON: Thanks, Janis. Thanks, Berry, for the presentation. That was useful and informative. Two comments come to mind quickly just looking at that. In Phase 1 we ran out of time to get input from DPAs or any kind of outside authority. We discussed sending the initial report to the European commissioner, DPAs. I think there was a desire to do that but we just ran out of time. We didn't get to that. I think that was a missed opportunity and I'd like to see us try and take that on this time around. I know there's talk about the strawberry group and maybe that can be accomplished as part of that effort. But I just want us to take that into account and that may have some ripple effects on the timeline.

The other thing was we had outside legal counsel and some of that advice came back after our final report was final. Again, we were overcome by events. We were working against a hard deadline. We also had a Phase 2, so we accepted the fact that we were getting legal advice after the fact. But I want to make sure we're counting for that in Phase 2 here and make sure we're baking in time to get legal advice in a timely manner, so that we can incorporate that into our final report.

So, just two quick hits from looking at that timeline. Those are two things that maybe we want to take into account and make sure they fit into your timeline.

BERRY COBB: They are on the laundry list.

JANIS KARKLINS: There is a reason why I'm suggesting to think of our activities to the September meeting because we're learning by doing and we're adjusting our expectations also as we progress. Though I must say, I hate to see 3% delivery after three months activities. I was told by staff that this is nothing exceptional because I need to look to those two green squares which are on the right-hand side from 3%, but I can tell you 3% hurt my pride. And you know nothing is worse than wounded pride. So, I hope that we will be able to demonstrate more delivery in percentage terms by September and that is my expectation or my goal.

Actually, your statement brought us to probably outstanding issues that we need to discuss. First is on the representative legal committee that we have constituted. In order to launch activities of this representative legal committee, we would need to look for a moderator of the conversation. I would like to say, at the beginning, I am not a lawyer and I would not really want to go into that business of moderating legal discussion. And when I look to the list of the delegated members and thought who would be the possible moderator, I discovered that basically everyone could be. But then when we come to practicalities, probably the most, let's say, neutral, if I may say, in the respect without the least maybe interest behind a presentation in that group would be the board liaison. I would suggest that Leon, if he would accept, could be the moderator of this representative legal group which then would work on all legal issues that have been already prepared by the staff, as well as that came out from our conversation Tuesday and today and would prepare material for consideration by the team as a whole.

So, my question to the team is whether that would be acceptable as a proposal, that Leon, should he accept and should team is in agreement, would act as a moderator of the conversation of this representative legal committee. I see nodding. Leon, you nod, too. Then, by everyone nodding, we are in agreement that Leon would act as a moderator of the representative legal team. We also would organize the work of the team together with staff support as required. So, thank you.

Another outstanding issue was what Marc suggested in the morning session, that we should talk a little bit about engagement with the strawberry team, what shape that could take. Marc, if you have some ideas, it would be now the right time to outline them and see reaction of the group.

MARC ANDERSON: Thanks, Janis. I do note the time here. There's not a lot of time, I don't think, for substantive discussion but maybe I can tee it up for future consideration and discussion. My thoughts or the reason why I raised my hand was really because of Georgios's intervention in chat. I wrote down what you put, so I'm going to quote you. "How do we move on and get the maximum from our interactions with DPAs?" We did not answer that. I thought that was a valid point.

We have opportunities to interact with DPAs and we have this interaction today from the strawberry group where we heard about what ICANN's efforts are in interacting with the EC, and potentially, DPAs to try and get additional information that can help guide our work.

Based on the conversations that we had following the strawberry group's presentation, I would say that we're probably [not] all aligned on what the best way forward is. So, I thought maybe a little more discussion on what this group wants to get out of an interaction with the strawberry group, how best we can accomplish that, and what ultimately an interaction with the EC or DPAs would look like. Hopefully, that's enough to tee up at least the thought process. I know we're eight minutes from our end time, so being aware of that, I'll just throw it back to you.

JANIS KARKLINS: Thank you. Georgios, your hand is up.

GEORGIOS TSELENTIS: Yes. On the same page as Marc here. He talked about missed opportunities and it's the same thing as with the legal questions. I think trying to phrase the perfect question of trying to see the perfect model at this time before and 100% agreed before we put in for at least an opinion or something to help us move faster, I think it's going to delay us.

I believe that we should go on with whatever the community can provide with us. As I said before also with the legal questions, I see a lot of value for professionals that can give us also the background knowledge about what is happening on the issue for the topics that we are trying to ask their help.

The same with the strawberry group. I think we should not have so much mistrust about what is behind and try to find out how to interact with those and get at least any answer from any question I find useful at this point because it helps us narrow down and move faster.

So, maybe it would be good that we consider – instead of freezing those things for the indefinite, try to make a plan how we get the maximum of this.

JANIS KARKLINS: Thank you. I think we have, as I mentioned in the morning session, we have this open invitation of CEO to provide list of policy questions that we would need to ask. I hope that our conversation Tuesday, today, would bring out some of those questions. I think one we have, on the liability issue of requestors.

I do not think it would be wise simply to bombard the DPAs with whatever questions we have. I think we simply need to develop those questions that they would be useful and they would help us to move forward. Otherwise, we may have opposite reaction, if they would be stupid questions. Sorry that I'm using that word.

So, they need to be well-crafted, thoughtful, which would really help us in our thinking and one on responsibility I think is really the one that should be asked as quickly as possible.

So, what I would suggest on that, if Marc or Georgios or anybody else would like to give a three or four bullets of questions that could be asked, we could [inaudible] online conversation about it and see what will come out from that conversation in terms of what are these policy questions that could be asked to DPAs. Otherwise, the legal committee will certainly bring up a number of questions that will be formulated also, not only [Burton Berg] but also probably for the DPAs. Would that be okay. Marc?

MARC ANDERSON: Thanks, Janis. I guess I'd be happy to work with … I think you're proposing maybe a starter thread for a discussion point and I think I'd be happy to work with Georgios to maybe get that started. I think we can coordinate offline and propose something back to the group.

JANIS KARKLINS: Thank you. Then we have remaining minutes to go through required things. So, next meeting is scheduled on Thursday. The team meeting is scheduled on Thursday 11 of July at 2:00 PM UTC. On Tuesday, the 9th of July, we are proposing to have open-ended call on priority two, items on accuracy and ARS. So, Tuesday's call would be to go through the worksheet that is in public domain already for a while and to try to finetune that worksheet in a way we did with the other priority two worksheets. So we will use the same methodology as we used before. Probably Caitlin will be taking the pen and then walking us through the worksheet as she ably did it before. So, that is proposal. No other meetings will be scheduled that week. The week after, there will be another team meeting.

With this, I would like also to call on Caitlin maybe to recap the action items we agreed during this meeting, please.

CAITLIN TUBERGEN: Thank you, Janis. The first action item would be for the EPDP support staff to send out the master template which has been updated, and all those who volunteered to draft additional use cases, please use this template. Additionally, the deadline for submission of any additional use cases is next Friday, July 5th.

Marc Anderson and Georgios to propose a few bullets for potential policy questions to the DPAs, which can be circulated to the list for further discussion.

And as a reminder from our last meeting, any groups that intend to submit early input should do so before July 8th.

JANIS KARKLINS: Thank you, Caitlin. Let me maybe very briefly to say about September meeting. We had the conversation. Meeting will take place in Los Angeles at ICANN headquarters. We would start on Monday, whatever time is normal for starting meetings in ICANN headquarters, 8:00, 8:30, 9:00? Around that, which means that everyone would need to fly in on Sunday. Since that will be the case, maybe one can think of legal committee meeting, for instance, on Sunday for a certain period of time, just a face-to-face interaction. That might be helpful.

Also, we were told – or I was told – that ICANN generously could open some bottles of wine for us that Sunday night. So, we will have maybe some icebreaking event or warm-up event and then we would start on Monday.

We would go through Monday, Tuesday, and Wednesday and I would like to say that please do not plan departure before the end of the meeting and we will try to plan end of the meeting at the time when people can reasonably leave Los Angeles if they want to catch the flights to the east coast. I'm thinking something like 3:00-ish end of the meeting that people can still fly out on Sunday to reach east coast if need be.

But please, we need to maximize our face-to-face time, especially that we're planning to bring facilitators the same company that facilitated our conversation during the first phase. Really, we would like to accomplish as much as we can in that face-to-face interaction.

So, this is as far as I can say at this point for September meeting but that is just to give you an idea what is [inaudible]. So, with these words, I am looking if somebody wants to say something good at the end.

So, in [inaudible], I would like to thank all of you for – Marc, please.

MARC ANDERSON: Something good.

JANIS KARKLINS: So, I would like to thank you for your active participation and constructive contribution. Thank you, staff, for supporting us in our activities. We [inaudible] rest of the day and we will come back on 11th of June. Thank you.

[END OF TRASNCRIPTION]