MARRAKECH – GNSO-EPDP Phase 2 Meeting (1 of 2)
Tuesday, June 25, 2019 – 08:30 to 15:00 WET
ICANN65 | Marrakech, Morocco

UNIDENTIFIED MALE: It is Tuesday, June 25, 2019 at ICANN 65 in Marrakech. This is the GNSO EPDP Phase 2 Meeting (1 of 2) at 8:30 in Tichka.

RAFIK DAMMAK: Good morning, everyone. We will start in two minutes. I would like to ask the EPDP members to take their seats so we can start on time.

Okay. Good morning, everyone. I think it's a good time to start. Let's start the recording first. Okay.

Thanks, everyone, for joining this session for the EPDP team today. You can see the agenda is shared in Zoom. We'll start with the first item to have some introduction since we go to new members joining the EPDP team. So, let's start first with the roll call, starting from James, to introduce themselves and their affiliation.

JAMES BLADEL: Good morning. James Bladel from the Registrar Stakeholder Group.

MATT SERLIN: Good morning. Matt Serlin from the Registrar Stakeholder Group.

OWEN SMIGELSKI: Owen Smigelski, alternate from the Registrar Stakeholder Group.

MARC ANDERSON: Good morning. Marc Anderson from the Registry Stakeholder Group.

KRISTINA ROSETTE: Christina Rosette, Registry Stakeholder Group.

MILTON MUELLER: Milton Mueller. You all know who I am.

AYDEN FERDERLINE: Ayden Ferdeline, Non-Commercial Stakeholder Group. And we do have a few other members that will be here shortly.

AMY BIVINS: Amy Bivins, ICANN Org.

DAN HALLORAN: Dan Halloran, ICANN Org.

TRANG NGUYEN: Trang Nguyen, ICANN Org.

CAITLIN TUBERGEN: Caitlin Tubergen, ICANN Org.

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

BERRY COBB: Berry Cobb, consultant for the GNSO policy team.

RAFIK DAMMAK: Rafik Dammak, the GNSO Council liaison to the EPDP.

BEN BUTLER: Ben Butler, SSAC.

GREG AARON: Greg Aaron, SSAC.

MARK SVANCAREK: Mark Svancarek, Business Constituency.

MARGIE MILAN: Margie Milam, Business Constituency.

BRIAN KING: Brian King, IP Constituency.

ALEX DEACON: Alex Deacon, IPC.

ALAN GREENBERG: Alan Greenberg, ALAC.

GEORGIOS TSELENTIS: Good morning. Georgios Tselentis from the GAC.

UNIDENTIFIED MALE: Good morning, everyone. I'm [inaudible] from the GAC.

RAFIK DAMMAK: Thanks, everyone. So, first, we'll come to all the members on the Internet that they are also observing these deliberations. Just as a reminder, only the representative or members to the EPDP are sitting at the table and they are those who can speak on those deliberations.

Also, maybe a reminder for the audience about what we are doing currently. We started phase two and we are mostly discussing about the system for standardized access and disclosure to non-public registration data. So, this is our focus.

What we are also trying to do for today is to try to begin with a real use case so we can learn more about the approach we are going to follow and see what we need to adjust or tweak on that model. We will start with a very real case that was [inaudible] by Thomas who has just joined us now. Yeah. Just [not to put him on the spot]. So, we will try to go that use case I explained and see what we can do. I really want to ask everyone to be patient and let's try something in the beginning so we can learn more. There is always that opportunity to make changes when it's necessary. So, I really ask you to be open to that.

Starting from there, also, we want and based on what we discussed on our last call last week is to develop multiple use cases for each lawful basis. So, we hope that we can [inaudible] lawful basis later on.

I think this is the overview for today. If there is any question or comment, it's a good opportunity to do so now. Okay. I guess we can move probably to the next item which is about the early input received from the SO/AC [inaudible] which is I think the part of the process of any PDPs to get input in the beginning and we had that

for phase two. So, maybe moving here to Marika just to ask which group they shared their input, submitted by the deadline, so we can start from there to discuss how we will deal or how we will process those input and use them for our deliberation. Yes, Marika?

MARIKA KONINGS: Thanks very much, Rafik. By the deadline of 21st June, we had received input from the Registry Stakeholder Group and the Registrar Stakeholder Group. Staff created an early input review tool. That's basically modeled or should look familiar based on the public comment review tool that we've used on previous occasions as well as we've organized the input received in line with the categories of the different charter questions that were specifically put out for input.

After that, we also have received input from the Business Constituency. We've updated the [comment] review tool and all those documents have been posted on the Wiki.

I'll just note that I think we've received two different types of input from the different groups. Some of the comments are really focused on the substance or responses to the charter questions, while others are more focused on potential additional questions that need to be considered or modifications on the existing

charter questions in the form of clarifying language that has been suggested to be added.

It would probably be helpful to know for the group what other submissions, if any, are still expected. As you probably know, there's an obligation as well for the group to review this input, consider it and respond to it or indicate what has been done with it. So, the group may also want to start discussing how you would like to proceed with that. It is already a pretty lengthy document because of course quite a number of charter questions and we already have input from three groups, so it may be worth it for the group to consider how to factor that into your work plan and what is the best method to deal with it.

As you may recall I think in phase one, we had some small teams assigned to review comments and then make recommendations to the group for how to deal with them. Obviously, that's something you may want to consider here as well. There are other approaches you may want to consider, too, so we just want to put this basically on the table and have your input.

RAFIK DAMMAK: Thanks, Marika. So, just before opening the queue, for those who want to intervene, please use Zoom instead of using the card. It's more easier to see the order and to not miss anyone. Any question, comment? Yes, Marika?

MARIKA KONINGS: Just for those desperately now looking for the Zoom room, you have to go to the ICANN schedule and then for this meeting you'll find a specific link. This is not the link we typically use for our calls.

RAFIK DAMMAK: Okay. Kristina?

KRISTINA ROSETTE: Thank you. I do intend to follow your instructions. I'm just having technical issues. I think it will be helpful for us as we discuss how we want to go forward with the early input review analysis and consideration if the groups who have not yet provided their early input could self-identify and indicate to the rest of us when we could expect to see that. Thank you.

RAFIK DAMMAK: Okay. Thanks so much, but just again, please use Zoom if you want to intervene, but okay for now.

UNIDENTIFIED MALE: Just responding to Kristina's point, the ISPs haven't yet submitted their early input. I expect that to happen within the next week.

RAFIK DAMMAK: Okay, thanks. Any other group that they are planning to submit? Hopefully as soon as possible. Ayden?

AYDEN FERDELINE: The NCSG will submit something early next week.

RAFIK DAMMAK: Georgios, please go ahead.

GEORGIOS TSELENTIS: The same for the GAC. We will submit in a week or two.

RAFIK DAMMAK: Okay. So, we have [inaudible] in when we will get this input to review them. Yes, Alex?

ALEX DEACON: It's Alex from the IPC. Yeah. We hope to have our as early as possible next week.

RAFIK DAMMAK: Thanks. Any other comment or question on this? So, I guess we will wait for other groups to submit their input. Hopefully, as soon as possible so we can include that in our work plan and to review

it in a timely manner. Okay. Before moving to the next agenda item, I was going to ask you, Marika, if you have anything else to add.

MARIKA KONINGS: I was just wondering if we can set a firm deadline, and probably looking at the GAC who I think has given the date that is probably currently the furthest out. But if there's a way to have a firm deadline for this, otherwise there's a chance that this is dragging on and the group may have already moved forward, and then looking back at the early input may not be in synch.

RAFIK DAMMAK: Okay. So, taking into account that probably people are traveling and [inaudible], but still, we need to get that as soon as possible. Let's say the 8th of July which is a Monday, so I guess fair time for all groups to make it. Any objection? Okay. So, let's go with 8th of July. So, I guess we can move to the next agenda item.

Sorry, James. You are following the rule and I missed you. Please go ahead.

JAMES BLADEL: Just a quick note that yesterday during the GNSO Council working session, there was a lengthy and spirited discussion about the

pace of work that this group is – whether or not it's hitting its milestones.

I just want to point out that we have a couple of groups that worked very hard to get their submissions in by the deadline and we have a couple of groups now that have not and that is part and parcel of part of the delay. So, I just want to make sure that when we are … I'll just say it. When we're laying at the feet of contracted parties for this group moving too slowly, that it's contracted parties that submitted their feedback on time and by the deadline. And I'm not calling out the rest of our colleagues here but I'm just trying to draw – put a spotlight on the fact that can we at least get some credit for that? Okay. Thank you because we certainly are held up often as the poster children for slowing down the work, but yet, we were the only ones who did our homework on this particular case. Thanks.

RAFIK DAMMAK: Okay. Thank you, James. Sorry, Alex, I missed you. Please, go ahead. Alex first.

ALEX DEACON: I already did. I'll take my hand down.

RAFIK DAMMAK: Thanks. Yes, Marc?

MARC ANDERSON: James, thanks for not slowing us down this time.

RAFIK DAMMAK: Okay, guys, guys, guys. Let's not go into this.

UNIDENTIFIED MALE: When you submit yours, you can talk.

RAFIK DAMMAK: Okay. It's not a contest.

UNIDENTIFIED MALE: Ours is submitted. It's just not posted to the list I guess.

RAFIK DAMMAK: Okay. So, it's not a contest. I think we are all doing our best here. So, I guess we can move to the next agenda item if there is no further comment. Marika, can you share the agenda again?

So, for this agenda item, we will continue what we started previously in the last EPDP call and continue the deliberation of all the SSID topics. So, what we will try, as I explained in the beginning, is to start from a kind of use case, and here it's the use

case that was proposed by Thomas. So, I would like to ask Thomas just to give a really brief overview. I think that we introduced before, but just for now as we are going to spend the day working on this, just to remind everyone and give the main highlights.

THOMAS RICKERT: Thanks, Rafik. Just to be clear, you don't want to discuss it now, just to introduce it at the moment or …? Because you asked me to keep it very brief. Do you want to open it up for discussion? In other words, how long do I have?

RAFIK DAMMAK: Okay. Yes. The idea I think is really to start first to just kind of overview and you can take your time. I'm not asking for two or three minutes, just five or ten if it's needed. But then the idea is really that, after we go through the time plate and try to ask input for each entry. So, we will have some discussion.

THOMAS RICKERT: That's fine. So, this will then be partially repetitive of what I discussed during the last call, to take the entire group of attendees with us. Yeah. Let's dive straight into it.

The idea for this document was to hopefully have the group move forward and agree on a methodology to advance our thinking and delivery of a work product for the universal/disclosure model.

What our group has found in the discussions over the last couple of weeks, that we couldn't really agree on how to proceed. So, there was an attempt to take purposes as the starting point for our discussions and the group didn't like it and then I think we wanted to use requestors as a starting point and the group didn't like it. Then, I said, okay, I'm going to potentially take the heat for making another suggestion and that is start with a case which we frame the least legalistic as possible, with simple questions. Who is asking for what, for what reason, and what shall the requests return? And a couple more points. So that we will basically have a list of simple questions – not legal questions, but real-life questions, if you wish – that you can answer in plan language, but that will still contain all the necessary components to make a valid legal case.

Good news is that I think I was only shot down by half of the group but some liked it. There was some comment and we had some discussions around it. I got feedback from all [inaudible] in our team. So, I think we can take this document to the next level. So, this is not a final work product but it's just the starting point of a bigger conversation.

I should also point out that this is for our group to learn and establish a methodology rather than trying to nail down the specific case. So, it's still a work in progress.

But the idea is, at the end of the day, that we would agree on the building blocks, if you wish – the component parts, the integral parts – that you need in order to make a solid legal case for a [UAM] for different types of requests that might be directed at the operator, whoever that might be ultimately, of handling the requests and that we could then split into subteams that could work on cases of their choice. And we could then tell them, "Okay, you do your homework, if you wish. Just make sure that you populate all the fields, and then at the end of the day it adds up. But we don't really care whether you then take your favorite purpose as a starting point or whether you take your [inaudible] legal basis as a starting point, as long as we have all the components in place." So, that's the thinking behind it.

This document shows a use case which is very narrow but we might be able to work a different more or less narrow cases, and at the end of the day, we might be able to group them, put them back together. We might establish that for certain use cases we can't standardize things. But I guess we need to go through the thought process, as in this methodology or comparable in order to be able to make substantive progress that hopefully everybody can understand.

So, this particular use case is limited to a trademark owner who sees that the trademark that he or she owns has been infringed upon with a domain registration and who wants to know who's behind that domain registration in order to determine whether it makes sense to take legal action against the registrant. At the moment, as you know, most of the data is redacted, so we're talking about how to enable the disclosure of non-public registration data.

So, the first question is what is the user group that qualifies for this use case? So, that's trademark owners, their attorneys or agents. And I should say that, with agents, I think this is a term that is not used in the same way around the globe, but the idea behind that is that Germany, for example, the legal profession is quite a regulated profession so it can't be just anybody who puts a sign "agent" above their door. But we need to come up with a definition that narrows it down so that only people who have to follow certain standards can issue such requests.

Other intellectual property rights, such as patent or copyright owners, are not considered here. Ideally, it should go without saying but I just want to manage expectations for this use case. We're not talking about copyright infringement taking place through the registration of a domain name or through content that is made available via a domain name, but this is just somebody objects against a string that has been registered.

Why is non-public registration data requested? We basically take language from the GDPR in the [inaudible] that the reason for requesting the data is in order to take legal action against IP violations through the violation of a domain name. The GDPR enables that data can be processed in the pursuit of civil claims or in the defense of legal claims. So we can add that up a little bit as appropriate to cover what's permissible explicitly under the GDPR.

Then we talk about the lawful basis. I'm not going to read through this. But basically you find in here a rationale as to why disclosure can take place in these kind of cases under 61F of the GDPR and you might remember that we have a catalog of legal basis in article six. And as the case may be, we need to go through all the legal basis and check whether of this, if any, are applicable to make a solid legal case for the type of disclosure in question.

On this point, I should add that I only mention 61F. And I guess this is important for our discussion because you can split the disclosure requests into several processing activities. You can split that into the request being submitted, the disclosure potentially taking place. And the requestor also needs a basis for accepting the data. So we can make this three boxes but I conflated it here for the sake of keeping things simple. But we will need to have a broader discussion about the legal basis for other use cases.

Then, general safeguards. We're at point D now. On that point, I should say we have general safeguards that we need to discuss that need to be followed by every type of requestor for every type of use case. Basically, that would be things that you put in front of the bracket that are applicable to everyone. We're going to discuss about safeguards for a particular use case in a moment and these might vary. So, law enforcement might need to have different safeguards in place than trademark owners asking for data – or none or what have you. But that needs to be looked at differently.

So, this is more about the general safeguards for an accreditation of whatever shape or form. Can you scroll down a little bit, Marika or Caitlin?

Basically, it says that only accredited users may request only current data. So, no data about the domain history. And what's important to note here is that these points basically reflect – at least my understanding, but that's for discussion – of what's within and without scope of this EPDP team.

Many of you do know that there are commercial vendors who have databases of all sorts of registration data where you can do a lot of great stuff. You can do reverse lookups. You can do Boolean searches. You can look for e-mail addresses only and check what other domain names are associated with a particular

e-mail address. You can take the tech-c as a starting point or the billing-c. You can do everything, more or less, that database search makes possible.

But all these additional queries are nothing that ICANN or the contracted parties have previously offered. And it is my understanding that it is the task of our group to make compliant what ICANN has previously offered, or a variation thereof. Not to introduce additional services. And this is why you find here a clarification that there is no Boolean search functionality, that there is no bulk access, that you can only issue sequentially your disclosure requests, that you can only see data for a single domain name at the same time. You can't look for other data elements other than the domain name and get something returned. No reverse lookups.

And as long as we don't have a centralized system in place, you need to go to the contracted party that actually holds the data and we might need to have volume limitations, slowed down response times or CAPTCHAs implemented to avoid mass lookups or automatic lookups that basically allow for reverse engineering of the entire database of registration data. But we'll get back to that and see what's required and if this set of criteria is actually meeting our purposes or meeting our requirements.

Then, we need to discuss about data elements typically necessary to achieve the goal, achieve the purpose. In data protection terms, we can't look at what is nice to have or what the parties would wish to have or what makes it easier for parties to achieve their goals. But the starting point is use the principle of data minimization, use the principle of privacy by default and privacy by design, and basically start from there and then you can only justify the processing of data to the extent necessary to achieve that purpose.

And this is why we have to discuss if you want to take legal action against a domain owner for cybersquatting, what data do you need? We've [inaudible] already the [inaudible]. He's still partially alive, the tech-c, but we've stripped down the dataset for the tech-c. There's no billing-c anymore. But we still do have this limited data set for the tech-c and a set of data for the registrant, and the question is what data does the trademark owner need in order to perform the pursuit of – to go after the registrant to pursue civil claims?

That leads to the question: what data shall be returned? My take on this was to not disclose the data of the tech-c. To disclose the name, organization, and postal address of the registrant. I think it would make sense to make the e-mail address part of that set of data that's being disclosed but I think we should discuss whether fax number or phone number belong to that. I think it

can be defended either way but I think we need to put rationale into our report as to why certain data elements will be disclosed or not. And that's a discussion, again, that we need to have for all sorts of disclosure requests.

Then, we need to talk about policy principles or how an accreditation for this specific type of query is conducted. So, for this type of use case, we're talking about trademark owners that aggrieved by an infringing domain registration. If they need to have [inaudible] ownership of the intellectual property right, they need to have a letter of authorization from the rights holder. That would be a licensee, for example, who is unable to take legal action or it can be an attorney that has to present Power of Attorney, for example. Then we have the requirement agree to certain – to use policy, that they only use the data for legitimate and lawful purposes, as described above. That's an acceptable use policy or terms of use or whatever you might call them to be part of that. And if you don't play by those rules, you will be kicked out after a warning or without a warning. But that's the logic behind it.

Then, the requestor has to promise only to issue disclosure request pertaining to that particular narrow goal and where ownership of a trademark has been evidenced. They need to tick a box to agree to the terms of service. We need to make sure that – they need to promise not to abuse the data and help prevent

the abuse of data received. They will be subject to de-accreditation if they're found to be in abuse of the data and they need to fulfill certain transparency and accountability requirements such as documenting the requests that they issued.

Now, you can frame that differently but that's the main idea. Then we would have policy principles for authentication to be discussed and other factors that might be required to put into the document.

So, that's a quick run-through. I think we can now move to a discussion of the individual items. Rafik, do you want to chair this?

RAFIK DAMMAK: Okay. Thanks, Thomas. Yeah. The idea is really to … So, thanks for this introduction and explanation about the content. So, I think the idea is really to go through item by item and get input or questions. So, in the way that we can confirm those different entries for the template and see if there is any concern or agreement, so we can, with that, go into a [systematic] way to hopefully finalize this.

First, let's see if there was any question or comment to Thomas's explanation. I see that we have Alex and then Kristina. Alex, please go ahead.

ALEX DEACON: Thanks. And thanks, again, Thomas, for putting this together. I won't dive yet into the details but focus more on the template, the methodology for now. I have two comments/questions.

I guess the first is regarding how narrow we want each of these use cases up top to be, because what I'm trying to figure out is what additional use cases may need to be submitted after we go through this.

So, I agree that we should start with a narrow use case to focus on what we're trying to do here. But I guess the first question I have is, for example, this use case, does it allow for the investigation of trademark infringement or is it only specific to a request that requires some type of legal action as an end result? I'm just trying to feel that out. Why don't we just start with that for now? Then I have other questions later. Thanks.

RAFIK DAMMAK: Okay. Thanks. Thomas, do you want to respond?

THOMAS RICKERT: On this particular case, I tried to steal language from the GDPR to keep that part of our conversation least controversial. GDPR explicitly states, as you'll find in the box next to C, lawful basis,

that processing is recognized for establishment exercise or defense of legal claims and that would include the investigatory part. Whether or not we want to broaden the scope of this purpose here I think is up for discussion by this group.

Again, the idea just was to avoid discussion about scope before we have concluded our discussions on the methodology as such.

RAFIK DAMMAK: Okay. Thanks, Thomas. We have for the queue, Kristina, Milton, and then Margie. Alan?

ALAN GREENBERG: I assume you mean this Alan. I guess I'd like to understand better where we're heading with this. I understand and I support the concept of doing a few use cases and we'll try to learn something from it. I have a little concern, though. If the decisions we're talking about here are deemed to be policy, how do we handle – once this PDP is over, how do we handle new classes of whatever – entities, groups, people – that will need access, new use cases? Are we going to have to reconvene a PDP or are we going to have some method whereas this is done in a practical way? So, I'd like to know what the steady case is going to be and what are we targeting? Because we may be setting ourselves up for something which is just not implementable. Thank you.

RAFIK DAMMAK: Okay. Thanks, Alan. So, let's hear from others and maybe we can come back to that. Kristina?

KRISTINA ROSETTE: Kristina Rosette, Registry Stakeholder Group. I actually have some substantive comments, so I'm happy to yield if there are others who want to follow-up on some of the points that Alex and Alan have made.

RAFIK DAMMAK: Thanks, Kristina. We can come back to you later about that. So, Milton and then Margie.

MILTON MUELLER: Yeah. I'm focusing here on the concept of accreditation. I think it's interesting what he's proposed and I think I generally support this approach to working through these cases. But I think the key question is how generalized is accreditation? Who would do it?

So, for example, if Facebook comes up and says, "I've got 375 trademarks and I've got 420 agents working on this," do you accredit them in one swoop or do they do it individually with each request? Once they have done a particular request, do they have to go through that process again and again?

But the one thing I like about your concept of accreditation is that it can be withdrawn. It's an enforcement tool for abusing the data, abusing the disclosure process. Again, how do you think that would work? Those kinds of questions I think we need to discuss. I know that you don't have to have that all worked out in detail but I'm just curious as to how you would approach those kinds of questions.

RAFIK DAMMAK: Milton, I don't have a full answer for all your questions, nor do I have a complete answer for what Alan has asked rightfully. I guess we need to take one step after the other, though. I think what we should try to do with this is walk through the case from start to the end. Basically, to run through it as you would in a real-life scenario. What component parts do we need? If a requestor knocked at the door of the ICANN ecosystem, for a lack of a better term, before we have to find who is actually going to do it. Then that requesting entity would need to subscribe to certain terms. And we need to wonder about what should be in those terms. What are the [inaudible] conditions for being part of this game. Then we can work on, drill down to whatever level of detail is required to answer questions such as yours. How do you deal with onboarding more trademarks? Do we need to go through the process again?

I intentionally didn't want to burden this with all the details but we have the [high] priority accreditation, then we have the execution of the disclosure or the processing of the disclosure requests. And for that part, we are entering unchartered territory because GDPR does not explicitly state that we can use rules-based processing, that we can do a [high] priority balancing of rights that would hold water if ever tested.

So, I think we should play this through and try to get feedback from the authorities, ideally, on how they view this because there seems to be a political [inaudible] to actually making progress with this. And once we've gone through this once, then we can hammer out all the details. But I guess I' more interested at this stage in using this, more or less, as a feasibility study of how far we can go, if at all, with an accreditation.

RAFIK DAMMAK: Okay. Thanks, Thomas. So, we have Margie, Alex, and then Stephanie. Margie?

MARGIE MILAM: Hi. I think Milton raises a lot of good points. I'm commenting right now on the format, not the substance. One thing – and I think I'm confused with the format – is how does this feed into the purposes? Because at some point, we have to get to what the

purposes are. And while I understand that this is a very narrow use case, as Alex mentioned, there's probably a lot of other ones that will lead to IP-type claims and it'll take us forever if we go to this level.

So, I think it will take too much time to go at this layer of specificity and I suggest that we go higher and understand how it feeds into the purposes discussion.

But then the other thing, as you scroll down and Milton's questions and the ones about the safeguards, it's obvious we have to have safeguards. It's obvious we have to have some discussion about where we're going to land on accreditation and all the questions that Milton asks are correctly issues we have to address. And if we do it with every single use case, I just don't see how we'll get through this. It almost seems to me that some of those big concepts have to be discussed separately apart from the template. So, we kind of look at this template and look at it from an, okay, what's unique about the use case that we're looking at and some of the big questions about accreditation and safeguards we do in a separate discussion because I don't know that it'll be that much different for every single use case and it just seems like it will be repetitive.

So, those are my suggestions on the template itself.

RAFIK DAMMAK: Okay. Thanks, Margie. Alex?

ALEX DEACON: Thanks. I think that's a good question. I agree with Margie. But again, on the template, another comment I wanted to make is regarding this accreditation section. I'm wondering if it makes sense to split it up into requirements for the requestor requirements for how data is handled after it's – or if it's been disclosed, just to separate those two separate concepts. We could squish them together but it seems to make logical sense to make them two separate sections.

Again, I agree with Margie. Just thinking about this a little bit on the fly here, it may be that there's more commonality between how third parties have to handle the data if it's been disclosed across many use cases, whereas the requirements for the request may be different – and again, I think we'll have to go through this to understand – maybe different depending on the use case or the purpose. Thanks.

RAFIK DAMMAK: Thanks, Alex. So, we have Stephanie.

STEPHANIE PERRIN: Thank you very much. I actually have a contrary view. I'm delighted that we're getting down to concrete examples and I'm not convinced that the differences among the various use cases are going to be that profound. For example, de-accreditation. You need some procedures for that and some basic principles and it's going to vary slightly over the type of case, but not that much.

I apologize to Thomas if you talked about this and I was tuned out or under-caffeinated but the point I wanted to raise was the notification to the concerned individual whose data we're talking about and retention schedules. This is just me not being familiar enough with the GDPR to understand how long they have to exercise their access rights once the data has been given to the third-party and what you have to do in terms of notification. Thanks.

RAFIK DAMMAK: Okay. Thanks, Stephanie. So, hearing all the comments about using the template or not and all the concerns. I think having the template and starting with the use case is to – maybe also [inaudible] on what Stephanie said, maybe we can find something that a lot of commonality [inaudible]. There is not so much difference. Or maybe there are difference but the only way to do that is to start with the use case, because at the end, we are going to go to more high level. But it's more I think easier and I

think it's more practical to start with those use cases and see where there are the common area and the difference. And it's more easier than to outline the high level.

I don't want to get in this kind of discussion from where to start. We need to start somewhere and you have to fix one parameter so you can elaborate for the rest.

So, I think we can try and see. If it doesn't work, we'll have to adjust anyway. Sorry, Thomas, you want to add something?

THOMAS RICKERT: Yeah, just briefly in response to what Stephanie said. Certainly, we need to hammer out all the detail – information, [inaudible] 12, 13, GDPR and all that. That needs to be done properly.

I also agree that we might find that a lot of factors aren't the same for all use cases, yet we need to plow through all of them very diligently because the data set that's being returned or the nature of the data being returned might vary differently. IT security researchers might not need to know the real data of the registrant. They might be okay with pseudonymized data or somebody might just want to find out whether somebody is actually responsible for hosting a massive number of domain names for illegal purposes. So it might be good enough to return

a number. This e-mail address is associated with X amount of domain names, without returning any personal data.

So, we need to go through that differently. The responses might be different. I guess we're going to have a lot of fun discussing requests by public authorities because then we need to talk about the crime involved, so that you know potentially harmful data is being revealed for somebody having a parking ticket. We need to make sure that we have the safeguards in place, that people are not facing capital punishment if data is disclosed, because I guess that at least might not be prone to automatic processing. So, we need to plow through that diligently.

But I agree with most of what's been said. We need to have a great level of granularity first and then we might be able to compress it to a single set of criteria.

RAFIK DAMMAK: Okay. So, just a reminder. Please Zoom to be in the queue. It's more easier for me to manage it. Yes, Amr, I know that you come late but we agreed to Zoom to be in the queue. Okay. But for now, it's okay. So, Amr and then [inaudible]. But please really use Zoom. It's easier to see the order. Okay. So, you see the [inaudible]. Okay, so we have Hadia, Marc, and then Amr. I think, Kristina, you want to comment or it's an old hand? You want to come back to comment later?

KRISTINA ROSETTE: Well, once we start talking about substance I'd like to come back.

RAFIK DAMMAK: Okay. So, [inaudible]. Hadia, please go ahead.

HADIA ELMINIAWI: Thank you, Rafik. First, I would like to thank Thomas for this work. It's great. Definitely I do find using use case is a good approach because it enables us to define the users as this is how we would like to start. Then, from the uses, definitely we have the purposes and the lawful basis.

I do agree, though, with Margie that having too much details in one worksheet I think is not going to work. We could stay addressing one use case forever if we go into that much detail.

I think that we should follow the structure that we had in the beginning. So, I think that using the use case, defining the users, the purposes, and the lawful basis would be a good start and we stop there. Then, later, after we have all of our users, the purposes and the lawful basis for each, then we start discussing the second part which will be talking about the accreditation and the other necessary steps. So at least we end up with something with users and lawful basis for each. And after we have that, we start our

next step which is the accreditation and safeguards and everything else.

So, I would go for breaking the work.

RAFIK DAMMAK: Okay. Thanks, Hadia. Marc?

MARC ANDERSON: Thank you, Rafik. I guess I had a chance to sit back and listen to what a lot of people said. For the most part, I don't think people were disagreeing. I think Thomas is giving us a path forward that shows a lot of promise. So, thank you, Thomas, for the suggestion and giving us a little bit of a template here to maybe move forward on this.

A couple of points. Alan Greenberg raised at the beginning I think he mentioned what happens with use cases that we don't envision. I share similar concerns. I think if we turn this into an exercise where we try and identify all the possible use cases, that'll turn into an exercise in futility. But as Stephanie got to, I think we'll find that if we go through this exercise looking at a focused use case, I think we'll find that there aren't a lot of significant differences between the use cases. So, I think there's a lot of value in us focusing our attention on just one narrow use case and walking it through from start to finish and flushing out

what are the answers to all these questions that we raise in this discussion.

Keep in mind, ultimately our goal is to develop probably recommendations. So, I think the last question on this worksheet are: what are the policy recommendations we would need to accomplish this?

So, I think starting with a narrow focused use case rather than trying to boil the ocean and deal with all the problems, all the use cases, all the challenges facing us is a good path forward and I think a lot of what I've heard from people supports this. I think it [inaudible] the potential of possibility to give us a path forward.

RAFIK DAMMAK: Thanks, Mark. Amr?

AMR ELSADR: Thanks. I'd like to go back to the issue of accreditation. I think I mentioned this during last week's call. And this is a question, really. Is there anything in accreditation, what is required to accredit a user, that cannot be included on a case-by-case basis with each disclosure request and what purpose does accreditation or what purpose is it meant to serve?

Some of the thoughts I've been having on this issue is some mark holders might lose their marks under certain circumstances. How would we know this happened if they're accredited?

The same thing concerning agents or attorneys acting on behalf of a marks owner. The authorization to act on behalf of the trademark owner might be withdrawn from an attorney or an agent. How would we know this, the agent or attorney would remain accredited? These are just questions I have right now and they're not specific to this use case. They're concerning accreditation in general. Are these things that we need to think about? And if there are any preliminary thoughts on this now, I'd like to hear them. Thanks.

RAFIK DAMMAK: Okay. Thanks, Amr. So, it's kind of the substance. I know that, Thomas, you want to respond to this.

THOMAS RICKERT: If you'd like me to. I think, Amr, those are operational details that need to be worked on. But I could think of an accreditation that is not for [eternity] but that is for a specific period of time, potentially associated with an accreditation fee for undergoing the initial accreditation perhaps deterring bad actors if they have to pay a little bit for the admission to the system. And then you

might have a renewal fee for that. So, agents who are no longer qualified to act on behalf of the trademark owners would then not be eligible for renewal and that would also go into the terms of service for this type of activity, so that they would have to guarantee or warrant that they are still authorized to do that.

RAFIK DAMMAK: Thanks, Thomas. Ashley?

ASHLEY HEINEMAN: Thanks. I apologize to Kristina. I know she's trying to get to her substantive questions but I am going to talk about just a methodology we're using here. I do think – and I believe my colleagues from the GAC agree with me – that this is a good exercise, if nothing else, just to go through and identify the issues that we need to talk about.

But one thing, as a GAC, when we've gone through this document is that there's a lot of information here. That's good to a certain degree, but I think it also begs the question again of what's the scope of our group and what are we best suited to cover and not cover? And I think we need to be really mindful of that as we go through this because I think there's a lot of cases here that it's really not worth us having the conversation because it's not really within our remit to be discussing.

Just to use as an example – and I'll be happy to refer to my European Commission colleague with more authoritative details – just going through the lawful basis, what are we talking about here? Are we talking about the lawful basis for the requestor? Are we talking about the lawful basis for whoever is the controller of a disclosure model? Are we talking about lawful basis of the contracted parties? Because it will be different. And it's not clear to me that we should even be talking about the lawful basis of the requestor making a request because that's their responsibility and are we going to be questioning their lawful basis or is that something that we will be … That's a good question we should be asking ourselves, then, because how are we defining the balancing test? What are we balancing? And it's not clear that we need to be looking at everything because there's different parties and they have different responsibilities. And what are we talking about here within the EPDP and what's a responsibility of other parties?

If you're having a model in which you have requestors making the request and self-identifying themselves in user groups, isn't it their responsibility to be defining for themselves what their lawful basis is? Because they will have responsibilities and liability as well. So, why are we taking it upon ourselves to be [inaudible] what their lawful basis is?

So, I just want to make sure that we are all talking the same language, if nothing else, and that we understand what our exercise actually is.

RAFIK DAMMAK: Thank you, Ashley. Brian?

BRIAN KING: I agree that we want to be clear about what accreditation, what the concept of accreditation does for us and the IPC understands fully that just because you own a trademark does not give you carte blanche to anything, that all the requests need to be legal and need to meet all the safeguards that we need. So, I like the concept of accreditation if it makes something easier, if it gives us a better legal framework for this. But I'd like for us to think about what it does for us.

Then, to Ashley's point, we're kind of in a weird place because we're talking about the third parties purpose and the third parties basis for processing the data but the contracted party or whoever is the entity that transfers the data to that third party needs to be able to rely on their own legal basis for doing that transfer.

So, we're kind of in a weird place where we're talking about the trademark owner here but then that needs to be good enough – and I think this is where we can get some good legal advise. I can

tell you that I think it's okay and that the contracted party should be able to rely on that but you won't listen to me, so let's get some legal advice on that, so that we get the legal certainty and the comfort that the data can be transferred to the third party for that third party's purpose.

RAFIK DAMMAK: Thanks, Brian. Okay. Just to check, Hadia, is that a new hand? New hand? Okay, please go ahead.

HADIA ELMINIAWI: So, my understanding – and commenting on what Ashley was saying – that the purpose of the user … So, we define user and each user has a purpose. And the purpose of the user determines his legitimate interest, right? So, we need to determine the legitimate interest of a user.

But, the lawful base, is the lawful base of the processor for processing the data? So, the lawful basis is that of the controller or the processor. So, the processor is able to disclosure, the data, is able to process the data because of 61F or 61B.

So, the legitimate interests are related to the purposes of the users but the lawful basis is part of the processor. Or I don't know. Maybe someone else can. But that was my understanding from if

we say 61F, that's why the controller or processor is able to process the data, right? No? To disclose. No?

I'm now confused. I think we need to mention clearly the legitimate interest. I see no legitimate interest in this worksheet. And the balance is done … When you do the balance, how you do the balance? You balance the legitimate interests of both parties, right? So, where's the legitimate interest here that we are going to balance?

RAFIK DAMMAK: Okay. Thanks, Hadia. I know that Thomas was in the queue probably for something else but it seems that he wants to respond to your question.

THOMAS RICKERT: I guess our discussion shows, at least to me, 100% why we should go through this for each and every case. We're trying to put in front of the bracket all the bells and whistles that we can't possibly – at least I can process with my brain power.

So, for this case, Hadia, to answer the question, this includes 61F for the contracted party that can review the data based on 61F. And I mentioned in my opening remarks that we can split that as needed. So, we can split that into different processing activities for the disclosing part as well as for the receiving end for public

authorities – at least under German law is something called the [double door] theory where both the public authority needs a legal basis as well as the disclosing party. But let's discuss that when we get there.

This is the beauty of this case because it's so easy, because GDPR foresees that you can disclose the data if somebody fulfills certain criteria as outlined here. So, let's stay here. It's going to become far more complicated when we're talking about public authorities asking for data. I don't want to go there. I mean, I can illustrate that in a few minutes if you want to but I think we should really take one step after the other and it will be baby steps and you might be impatient. But I promise you, if we go through this once, then a lot of things will fall into their places.

HADIA ELMINIAWI: Thank you, Thomas. This was initially my understanding, so thank you.

RAFIK DAMMAK: Okay, thanks. Stephanie?

STEPHANIE PERRIN: I just want to strongly endorse what Thomas is saying. As long as we keep at the high level, we are chasing our tails because it's

only when we get down to the concrete bits that we are able to develop the procedures that will be reflected in the policy, and in some cases, this is iterative. I know people in this community think, "Okay, we come with a high-level policy here and then it gets implemented." No. We have to figure out what the required steps are so that we can include that in the policy before we toss this to the implementation committee.

So, I would strongly endorse us working our way through this asking the questions that naturally arise as to the legitimate basis for the request. We need to dispel the notion that a user has the same reason for a request for disclosure each time. These will be different each time. You could be coming in … I mean, maybe you are going to be dealing with an FBI agent that only does, I don't know, murder investigations. But that's highly unlikely. You're going to be dealing with a law enforcement community that are coming in with different basis for each request.

So, we've got to walk through the complexity of it to get out the other side of this tunnel. Sorry for the analogies that are fighting with each other. There's a train in there somewhere.

RAFIK DAMMAK: Thanks, Stephanie. Hope that we will see the light. Okay. So, we have Alan Woods and then Georgios, and after I want to see where we have agreement and move on. So, Alan?

ALAN WOODS: Stephanie took the wind out of my sails, to extend some of her metaphors. The train, with the wind and the sails. But I just want to again, because it seems to be something I have to say in every meeting at least once and I don't want to repeat what Stephanie said. But again, you're talking about trying to define people's legitimate interests. Nobody here will be able to define what that legitimate interest is. It is up to the requestor to define what their legitimate interest is in any given case. And that's why we have that issue then with defining different user groups, because again when we go back to the one which has been sent to me several times, is that the ice cream sales person, the person in the ice cream [inaudible] may have his legitimate interest and he may have a legal basis on a specific request. We will never be able to come up with those interests. I can see that we might be able to get ring-fenced concepts and that's why it's really important to go through what Thomas is doing at the moment because it just shows the steps that we will have to look at and the decisions and concepts that we will have to consider in every request, regardless of who it is or what legal basis that they're basically looking at. It's taking us through the intellectual steps that are necessary in order to get from the request to the release or the non-release in those cases. So, I full endorse Thomas. Thank you, Thomas.

RAFIK DAMMAK: Thanks, Alan. So, Georgios and then Ashley.

GEORGIOS TSELENTIS: Yes. I will try to go back to what Ashley said and the intervention of Stephanie. I agree with what he said. This discussion I think, for the legal basis, needs a clarification which for me is essential. When we talk Article 6 talks about lawfulness of processing, we are talking about lawfulness of processing activity, not about lawfulness of processing entity.

So, that's what we should bear in mind. And if we see the processing activities as separate, that we have a separate activity about the one who is disclosing, the one who is processing after the data are disclosed, then we have the legal basis that should be examined separately. This is what we said and this is what we have figured out when we went through the examination of the [inaudible] of the law enforcement agencies when they want to do that. They have their own legal basis for processing the data. But there is another story when we are talking about who is going to do the disclosure of this data.

So, every processing activity has its own legal basis and that's what we should not confuse. Thanks.

RAFIK DAMMAK: Thanks, Georgios. Ashley?

ASHLEY HEINEMAN: Somewhat of a separate point but just to respond to whether or not user groups are feasible or worthwhile. So, I think when we talk about the context of a unified access model and the whole purpose being to make an efficient, workable process by which to disclose information – at least my assumption has always been that in order to make this as efficient as possible you'll need to have categories of users who can self-identify, can be accredited, certified, whatever word we want to use, to make the process quicker and easier and more reliable and have more accountability associated with it.

Now, if that conversation is not suited for this conversation, I could handle that. But I think the problem is that there seems to be these off-the-cuff remarks saying that user groups just aren't possible and I think that's what makes a lot of people in this room concerned because I think part of what we want is to put all the cards on the table is recognition that user groups will be part of this process and this is one of the ways that we're trying to get that recognition.

So, if we can just agree that user groups will at least be considered as a possibility for some sort of disclosure model, then perhaps we can get over this hurdle to a certain degree.

RAFIK DAMMAK: Yeah. Thanks, Ashley. Just before moving to Thomas, I want to check, Alan, is it a new or old hand? Okay.

ALAN WOODS: I will take the opportunity, even though it was a mistake. Actually, I completely agree. I'm not saying that user groups aren't possible. I just think that at this particular moment in time, it is pointless starting with a concept of a user group will be treated and their request will be treated in this way.

I think we go through all of this, and ultimately at the end, as a matter of ease and a matter of implementing some sort of [UAM] if that is where it is going, then yes, obviously user groups make sense in bringing it all together and compartmentalizing aspects of this. But at the moment, we are not going to say a user group will have this response. I think we just plow ahead.

THOMAS RICKERT: Thanks, Rafik. I think, actually, you're making a good point. We should get clarity on the terminology that we're using and that will also help us understand what we're trying to achieve. I think we can do standardization by types of requests because there might be identical requests that require the same legal assessment. I'm not so sure that the user group can be lumped

together and then all sorts of requests that come out of this user group will be treated the same. I would rather make the distinction based on the request and to the extent by which a request can be categorized and standardized.

But I think, having listened to what many of you have said, what we will do after this meeting is change the contents of box C and clarify that this was meant to just cover the legal basis for the disclosing party, i.e. for the contracted party and as the case may be, if ultimately ICANN recognizes to be a joint controller, then it might be contracted parties plus ICANN that can use that legal basis.

But maybe just for the sake of shedding some light on this, in this case, it's relatively easy because the requestor will use 61F as a legal basis for making the request and the disclosing party can also use 61F for making the disclosure. But we will find cases where it's not congruent. So, if let's say from a home country, German law enforcement authority makes a request that might be based on the panel procedural code – so, they have the legal basis by which they can request data. But the disclosure is made based on 61C because the contracted party has a legal obligation or statutory obligation to fulfill.

So, we might find cases where it's not [common], and therefore I've lumped this together for the sake of simplicity, which in

hindsight was not wise. So, we will define this further and we will create different boxes for the legal basis of the requestor.

But the question is – and let me be very clear about this – I think it will be a massive undertaking if we actually wanted to assess or accumulate all the legal basis that national law enforcement around the world might have. So, I think we need to find wiser, smarter approaches for that other than trying to check the legal basis of the requestor if they are public authorities. And that might be by severity or nature of crime involved by the sanctions that might be involved and other points that need further discussion.

RAFIK DAMMAK: Okay. Thanks, Thomas. Georgios, an old or new hand? I think we have Alan and then James.

ALAN GREENBERG: Thank you very much. We keep on having people make the assumption that because we say someone is a member of a group that they will all be treated uniformly for every request they ever make from anyone in that group. All putting someone in a group says is we've identified what their nature is, not necessarily the nature of the request, nor how it's going to be handled. The same for use cases and the same for all sorts of other things. Let's keep

things orthogonal and talk about things separately and not presume they're linked to other things because that just gets us into problems. Thank you.

RAFIK DAMMAK: Thanks, Alan. James?

JAMES BLADEL: I'll be brief. Just listening to this conversation for the last however long we've been at this, I just want to emphasize that setting aside all the legal nuances that, from an operational perspective, contracted parties are going to need some boundaries around the different categories of requests and requestors and there's going to need to be some standardization of that request and the information that it contains and the format of that request, and ideally there would be as few of those categories as possible. So, I understand there's a danger in summarizing those and every request is like a snowflake. It's different and beautiful in its own way.

But when the rubber meets the road, we're going to need to break these down into chocolate, vanilla, strawberry and process them differently and the fewer the better. So, we're going to need to start moving towards practicality and not get wrapped around

some of these very important but very nuanced differences. Thanks.

RAFIK DAMMAK: Thanks, James. Thanks for everyone for all your comments and intervention. I think we have rough agreement that we should go with this approach. In terms of to help us to go through the details and see where there are common areas and think about the high level. We need to start somewhere.

On the other hand, I think there is some question more about the substance, so we can list them and come back to them later. I think accreditation and so on.

So, I think what we will do from now on is go through each entry and see if we need any change. Also, I think Thomas has suggested that maybe in terms of format we need to make some – you are suggesting to make some changes. So, we'll take that into account. Okay. Yeah.

We have I think that flexibility to change. At the end, all this material or tools is to help us to have this discussion and to find I think high-level principles and so on. I guess we will move with that approach. I think we just have 25 minutes left until the next break. So, let's go with that. And we start to discuss about the

substance. Kristina, I know that … [inaudible] your excitement. Please go ahead.

KRSTINA ROSETTE: Thanks. I think one thing that I'm struck by here and I will freely own my previous life as a trademark attorney, is that I think it is important that we include some type of requirement here that, after having received the non-public registration data through this disclosure process and that we do in fact have the time limit that Stephanie mentioned earlier, which was one of the things I was going to suggest, so I fully support that.

I do think we need to have some type of requirement of actual use of the data or an explanation for why, after having requested the disclosure and gone through the entire process, there was a decision not to use the data. I think that's something that should be tracked because what would be unfortunate is if we were to end up in a situation where, without such a requirement, a party would – the same party would – repeatedly request disclosure after disclosure after disclosure after disclosure, and then ultimately not use the data for the objectives for which it was requested and for which the disclosure was made.

And I certainly understand that there will be circumstances under which, for example, in this use case, after having received the data, the determination may be, actually, this is not a use that

violates our rights or, oops, this turns out that somebody in marketing who thought they were being helpful, actually, this is our own employee; we're not going to take legal action against them.

So, I certainly understand that there will be circumstances under which the data won't be used. But I do think there needs to be a requirement of either use or non-use and some kind of tracking of that. Thanks.

RAFIK DAMMAK: Thanks, Kristina. Any comment or question here? Yes, Marika?

MARIKA KONINGS: Thanks. Staff is trying to keep track of some of the specific suggestions that are going to be made. I just wanted to clarify, that is something that you would see being added to the safeguards category, right? Okay.

KRISTINA ROSETTE: Yes. And to be clear – and I think some of these categories are going to end up being very linked. For example, I would imagine that safeguards and maintenance of accreditation are going to be very linked in the sense that a particular user's continued

violation of the safeguards or failure to abide by them should ultimately affect their accreditation.

RAFIK DAMMAK: Thanks, Kristina. Just checking the queue. We have Brian, Margie, and then Alan Greenberg. Brian?

BRIAN KING: Sure. Thank you. I think a lot of safeguards are wise and that we should really consider appropriate and reasonable safeguards. I don't think that a requirement to actually use the data or to say whether you did or didn't use is a reasonable requirement. And I appreciate Kristina's feedback there. I'd like to know if that makes this more legally sound or if that concept is grounded in some other examples? Can we draw a parallel to some other case where that's necessary or appropriate? Again, I think a lot of safeguards are good but that one probably goes too far, in my opinion.

RAFIK DAMMAK: Okay. Thanks, Brian. Margie?

MARGIE MILAM: I agree with Brian. I think it raises a lot of issues about attorney-client privilege, all sorts of things that make it difficult to do what

Kristina suggests. But I do think that there should be safeguards and if there is accreditation, there's probably some sort of audit requirement along with it, so that things can be checked if it looks like there is abuse. But that's probably a little too specific, so I don't think that would work for us.

RAFIK DAMMAK: Okay. Alan Greenberg?

ALAN GREENBERG: Yeah. I think, despite the comments of my last two colleagues, the idea may have merit for this particular use case but I think it has absolutely no merit for a case of a cybersecurity investigator who is not really planning to contact the person but is trying to get information about it to establish, furthering what they're doing. It may apply in one case. It may not apply at all in other cases. I think we'd have to be really careful about doing that kind of thing.

RAFIK DAMMAK: Okay. Thanks, Alan. So, we have Mark, Alan Woods, Ayden, and Kristina. Thomas, also you want to intervene. Okay, Mark.

MARK SVANCAREK: I notice a common theme in the safeguards category, this fear that bad actors – I hate to use that term in this context – that

poorly behaved requestors will continue to be accredited and I think since we have not yet defined how accreditation is established, I don't think we can go into this detail yet but I think we should just have a working assumption that the credentials can be revoked and that there is some way for people to know when credentials have been revoked. And we'll have to get into that detail at some point but for the early stage of the conversation, I think we should just have a common understanding that if there is accreditation, it is revocable and that the knowledge of revocation is available. And I think that will help us move forward so we don't get hung up on that.

RAFIK DAMMAK: Okay. Thanks, Mark. So, just before moving to the rest of the queue, I know that all of you are making comments on different parts of the template but I think we should later on follow from the beginning and checking, [inaudible] where we have agreement or not. But for now we can continue and hear from everyone and we try to come back to follow in the template to be sure we are covering all the [entries]. Okay, so Alan Woods?

ALAN WOODS: Thank you. Just to go back to Brian's – I suppose to respond to Brian. Two things come to mind straightaway when he says: where would we find the equivalent to that in the law?

The first one is that, obviously, you cannot just process data with the intent of perhaps sometime using it. But that's a general principle in data protection. You can't just hold data because you might use it at some time in the future. That's been well-established. But I suppose, more specifically, if you are stating that, "I need disclosure of this data for this purpose," if you do not use it for that purpose, you no longer have that legitimate interest or that legitimate purpose, so you're actually negating the legitimacy of your request in the first place.

So, I think it's a very prudent suggestion that there has to be some indicator or some qualifier that you do use that data for the purpose which you have stated. Otherwise, it's removing that legitimacy.

RAFIK DAMMAK: Thanks, Alan. Ayden?

AYDEN FERDELINE: Thanks. So, firstly, I wanted to express my strong support for Kristina's proposal. I think it's an excellent one. And I wanted to respond to a comment that Alan Greenberg made.

So, all of these use cases are going to have different data elements that may be shared. So, in the case of a cybersecurity researcher that you referenced, there may not actually be any

personal information that is being sent to them. There may be. But if there is personal information – and I think Kristina's proposal makes perfect sense – there needs to be some safeguards in place.

But, again, if the use case varies and we're not talking about an address and we're talking about different data relevance, we might be able to do a different risk assessment and it might not necessarily be necessary for that particular use case.

RAFIK DAMMAK: Okay. Kristina?

KRISTINA ROSETTE: Thanks. So, just to respond to a couple of points. Alan, yes. I do think obviously the use requirement would vary, but I do think it is important that if we are establishing this process, this model that will be uniform and provide routine disclosure upon satisfaction upon particular disclosure requests, I do think we need to have that.

And Margie, with all due respect, I don't see an attorney-client privilege issue here. The entire purpose of the request is in order to take legal action against IP law violations. So, once that decision is made and the action is taken, then the fact of the action and the action itself will be a matter of public record. If the

decision is made not to take action because, for example, it's determined that it's a fair use, it's determined that it's a well-intentioned by misguided employee in the marketing department … My point is not necessarily to provide an elaborate explanation of the use or non-use, but I think there does need to be a statement of use or non-use, because otherwise, we could end up inadvertently creating and facilitating an environment in which some of the very objectives we're trying to achieve here are rendered moot. And I think that, to start out of the gate with creating potential loopholes I think would doom this whole effort to failure. Thanks.

RAFIK DAMMAK: Thanks, Kristina. Brian?

BRIAN KING: Thank you. I'm encouraged by this constructive conversation. I appreciate clarification on where you're coming from. I think that I assumed that a requestor of the data would be processing that data under an agreement that they would follow GDPR principles and not hold the data any longer than was necessary. So, where my confusion was that as part of the GDPR allows for establishment, exercise or defense of establishment of the legal claims, you may be processing that data to establish a legal claim that you may have or may not have. So, I think that if you were to

process the data to establish the claim, that doesn't obligate you to file a UDRP or to sue anybody. And if you're already agreeing that you won't hold the data any longer than you need it, I don't see what adding on some kind of additional assertion or proof does for it that agreement doesn't already do. That was my point. I thought it was extraneous. I didn't see the value in adding more to it.

RAFIK DAMMAK: Thanks, Brian. Stephanie?

STEPHANIE PERRIN: Thanks. I'm possibly indulging my love of complexity here but I was going in the exact opposite direction. It does seem to me that one of the merits of the TSG report is to demonstrate that we could actually be issuing tokens here – tokens that expire, tokens that alert others, cosigned by clients to assure that an attorney that professes to be investigating a claim for one client is not actually doing market research for another client. So, all of these things are possible under the TSG model with RDAP, so we can do it, right? I see Mark smiling. We can do it, right? And that's the kind of detail that we need to get into to make this enforceable under data protection law. Thanks.

RAFIK DAMMAK: Thanks, Stephanie. So, in the queue we have Alan, then Thomas, and Margie. Alan?

ALAN GREENBERG: Thank you. I just want to point out that if the information we requested happens to be contact data, that doesn't mean the only use of it is to contact the person. In Kristina's case, where you got the information and found out that it's a member of your own department and you decided to say, "Okay, we'll just tap them on the shoulder and tell them not to do that again," you used the data. You didn't contact … You may or may not have contacted them, but simply knowing who the person is gave you information which was sufficient to address the issue. And that's use. Just because it happens to be a phone number doesn't mean you have to dial it. Thank you.

RAFIK DAMMAK: Thanks, Alan. Thomas?

THOMAS RICKERT: Great discussion that we're having. I think with the interest in all the details, we can probably work on this EPDP for the next 20 years or so.

Joking aside, I think it would probably be helpful for us to make a distinction between what the legal basis for obtaining and retaining the data by the requestor is because the requestor needs to treat the data in accordance with GDPR, right? So, the requestor, who is an independent controller – on the disclosing end, you have … At least in my legal opinion, you have the joint controllers – ICANN and the contracted parties – that disclose the data to an independent controller who is the requestor and the requestor doesn't have the right to keep the data forever. So they need to check for what purpose they're requesting the data, and then once the purpose is fulfilled, they have to delete the data. And that is true for every type of requestor, whatever the nature of the requestor might be.

So, the retention periods that are permissible for the requesting party might differ from case to case. But that I think is something that we shouldn't be too worried about. We should be worried about the policy that should go into the accreditation. What does our group want to be the safeguards for volume-wise, time-wise? So we can differ from the legal basis and the retention period that the receiving end might have. So, I think we should probably focus on what we think is a good retention period, whether we think we need to build technical safeguards in order to prevent abuse of the data. And let's maybe focus our discussion on that, not that much on trying to determine or second guess what the

legal basis and an appropriate retention period on the receiving end might be.

RAFIK DAMMAK: Okay. Thanks, Thomas. So, we have Margie and then Alan.

MARGIE MILAM: I think one of the things, as related to the safeguards may address the concern, is that we include a representation that we're going to use the data only for the purposes stated and that's a contractual obligation as part of the accreditation that the requestor could be held accountable for and potentially lose their credentials if they're not complying with the contractual obligation. So, I think that's something that's reasonable to try to address the concern.

RAFIK DAMMAK: Okay. Thanks, Margie. I don't see anyone in the queue. I thought there was Alan. I think we have eight minutes left for this session and then we will have the break. It's good to hear all the different comments about the substance and we are taking a lot of them. But I think in the next session where we will continue this exercise, we will try to go by order. Why we are doing that is really to be sure or to make assessment that we all are in agreement, and if there is anything that we need to change or update, we will

do so. Hopefully, we finish this by today where we can continue probably to discuss other use cases and continue this approach Thursday. That's why I want to reiterate that.

On the other hand, it's more like an administrative matter. I was reminded several times to ask you guys when you speak to state your name for transcript purpose. Any other questions or comments? Marika, do you want to add anything?

THOMAS RICKERT: Rafik, I have a suggestion to make, if I may. When we reconvene and when we go into the discussion, can we maybe focus on the safeguards? I guess that would be a good use of our time to go through the safeguards. I would try to focus on three buckets. So, we have a priority accreditation safeguards, what needs to be the criteria for being accredited? Generally, the criteria that should apply to all requestors across the board. Then we have the special safeguards that pertain to a particular query and maybe that's something we can neglect for the time being. Then, we have the accountability safeguards afterwards. That would be transparency and documentation requirements and that will also be the things based on which we can then punish bad actors and kick them out of the system. So, over your coffee, maybe you can think about that. If you, Rafik, agree, maybe that would be a constructive way forward.

RAFIK DAMMAK: Okay. Thanks, Thomas. Just to be sure, you are suggesting that we jump into safeguards and start from there. Thomas, I was asking just to double check, to confirm my understanding. Okay. If there is no objection, we can do that. But I think, at the end, we will try to cover all entries, if we made it. Okay.

If there is no further comment … Brian, please go ahead.

BRIAN KING: Thank you. I want to support that we start with safeguards. Also, I want to make sure that we're looking at safeguards as GDPR defines them in a state of minimization and the privacy of all principles that apply as safeguards. I want to make sure that we are considering that in the procedural and operational safeguards, too.

RAFIK DAMMAK: Okay. Thanks, Brian. So, I guess we are all in agreement. Since we will spend the rest of the day continuing to [inaudible], I guess we can stop here and then reconvene at 10:30, having the coffee break. Before that, yes, Alan, you wanted to add something?

ALAN GREENBERG: Sorry. I did have my hand up. I'd just like some clarity. Where are we in the agenda? We seemed to have scrapped the agenda and done something different altogether. Are we coming back to it or where are we?

RAFIK DAMMAK: We are following the agenda. So, first was to go through the template and we had the discussion, so we will continue in the next session to do so.

ALAN GREENBERG: It doesn't seem to be following the words in the agenda but that's fine.

RAFIK DAMMAK: Okay. Thanks, everyone. Let's reconvene at 10:30 and let's have this coffee break. Thank you.

UNIDENTIFIED MALE: Rafik, could we agree that before we take breaks, we should actually accomplish something?

RAFIK DAMMAK: Okay, everyone. I think it's a good time to take your seat and we'll start in one or two minutes and resume our discussion. I'm asking EPDP members to take their seats. Thank you.

Okay, thanks, everyone. I think it's a good time to start. We already had an extra ten minutes to the hour break. Thank you.

So, as we discussed in the previous session, we will try for now to go through the template entry by entry. What was suggested before is that instead of starting to begin or start with the first entry, to start with the safeguards since we had several comments and discussions about that. But just before we begin I want to double check if we all are on the same page in understanding about starting with the safeguard. Okay. I see, Alex, you are in the queue.

ALEX DEACON: Thanks. I'm on the same page. I just want to make sure we are clear on exactly this use case on the top. I think my first intervention I mentioned I had a few questions around the scope. And based on conversations that happened earlier this morning, I think I'd like to suggest a clarification to that. I'll read it and maybe what I'll do is I'll put it in the chat, also.

Basically, what I would suggest is trademark owners processing data in the establishment exercise in defensive legal claims for

trademark infringement or cybersquatting. And this kind of ensures that there's ability not only to file a legal claim but to do the due diligence beforehand in investigating a potential claim. So, let me copy that in. Hopefully, it's not too controversial. It uses the language from the GDPR and I think it makes it clear that it's not specific to or, the end result, requires a legal action but allows for the investigation also. I'll just put that in.

RAFIK DAMMAK: Okay. Thanks, Alex. Okay. Let's check if everyone is okay with this change. Okay. Seeing there is no objection, I guess we can make this [inaudible]. So, as I said before. We agreed previously to start with the safeguard and just double checking here that we are on the same page, so there is no objection. Can we start with that one? Marika, can you move to the … Okay.

Thomas, without putting you on the spot here, I know that you introduced it before in the beginning the different parts, but do you want maybe to elaborate more for this one? If you want to add, based on what we discussed previously.

THOMAS RICKERT: For the safeguards? Yeah. I don't have a particular point to add but I think we should open it up for discussion and ask what

additional safeguards, if any, the group might wish to add to the list.

RAFIK DAMMAK: Okay. Thanks. Just wanted to double check if you wanted to add anything or maybe to elaborate but it's fine if everyone had a chance to review to see if there is any comment or amendment or addition to this. Okay. So, we have already a queue. I see Brian, Chris, and then [inaudible]. Brian, please go ahead.

BRIAN KING: Sure. Thank you. We have probably a lot to say here, but let's start with, one, I think general principle and then I'll make a substantive suggestion. As a general principle, I think that it would be prudent to add a safeguard that the requestor, or the third-party processor, agrees to process the data in compliance with GDPR , as a general matter. We can get into if we need to elaborate more specifically. But I think as a high level, we should add that.

Then, my substantive point is about only data of a single domain can be viewed at the same time. I don't think that's necessary and I can tell you from Mark Monitor's perspective, we have clients that regularly are monitoring and tracking infringements on a scale of tens of thousands of domain names at any given time that

are infringing and looking those up one at a time seems to be unduly burdensome. I'm not sure what the tradeoff is, if we have a sufficient legal posture to request the data for one domain name, I don't know how that becomes less legally sound if there's a lot of infringement happening. I don't think that's a prudent safeguard. I don't know what that does to safeguard the personal data or any personal data that's being processed, if there are a lot of domain names that are involved in the same instance. So, I would suggest that we remove that and that we add in the general safeguard about processing the data in compliance with GDPR.

RAFIK DAMMAK: Okay. Thanks, Brian. Chris?

[CHRIS]: Thanks. Just quickly to respond to Brian, if that's okay. On that single search, I'm trying to understand for this user case, the single lookups are not really going to be reasonable when you've got multi-case with multiple … Even if you're looking into the hundred or tens, it starts to become burdensome, really. So, I wonder if we can maybe expand the volume limitations to cover I think what is that query, to make sure that it's not an over-process and any data is required for the purpose or the user case. So, just tying down how we're requesting or how you're

requesting the data for that to the actual user case and purpose. That would be my view of getting around I think what your request [inaudible]. Does that make sense for you?

Then, one point for me that I think needs adding that's been missed is that only data requested is to be supplied. So, obviously what we don't want is the controller supplying more data than is being asked for. That's a definite safeguard that we want to put in place.

THOMAS RICKERT: Chris, can you move closer to the microphone? It's difficult.

[CHRIS]: Sorry, Thomas. I'll repeat that just in case you missed. Only data requested is to be supplied. Obviously, what we don't want is the controller taking a request and saying, "Oh, I also have this personal data," and sending that. I think it's really key that we limit any disclosure to what has been requested.

The second thing is that all data must be encrypted in transport. It's baked into the GDPR that all data is securely transmitted and I think that's a genuine one that should be there by default. Thank you.

RAFIK DAMMAK: Thank you, Chris. So, checking the queue, we have Milton, Mark, Margie, Thomas, and then Alan Woods. Milton?

MILTON MUELLER: Yes. I'm reacting to the statement from Brian about multiple requests. So, I'm not sure what he means exactly that you would submit a request for 10,000. I mean, I can see that if there is a particular trademark that is potentially infringed 10,000 times, which is perfectly understandable the way things could happen, I can understand you submitting 10,000 requests at once, I guess. But each of those requests would be a different registrant or a different record and you can really only look at them one at a time to determine whether they are – what you're going to do about this particular record or domain holder.

So, what we're getting at with this safeguard, which is very important to us, is this is not bulk access. This is not just give us all the WHOIS and we'll go rummaging through it to find out what we want. You're saying we have a specific infringement and there may be 10,000 of them but every request is essentially processed individually. I can't see how we could deviate from that.

Another minor point in terms of Alex's modification of the language, I have no problem with them, except I didn't quite understand when they say trademark infringement or

cybersquatting. What do the trademark people see as the difference between cybersquatting and trademark infringement?

UNIDENTIFIED FEMALE: If I could answer his question, trademark infringement involves I think using the actual mark itself, the string. So, you've got trademark claims that you would bring under this use case. Does that make sense?

MILTON MUELLER: So, would cybersquatting be a specific form of trademark infringement? Do you need both of those terms in there? That's all I'm asking.

UNIDENTIFIED FEMALE: I think, no, you're right. It's the same thing. I think the more correct word is trademark infringement and we call it cybersquatting but I don't know if it's defined … I don't know. Do you know, Brian? We'll look at that but I think you're right.

RAFIK DAMMAK: Okay. Thanks. So, you're agreeing to draw up the cybersquatting, so we need to take note of this change. And there is no objection. We are all in agreement here. Okay. So, next is Mark.

MARK SVANCAREK: Thanks. So, I'm sorry if this was explained earlier. Thomas, can you confirm when you say only data of a single domain name can be viewed at the same time, was that intended to be can be requested at the same time or was it to mean, as Milton was suggesting, that having requested a number of things individually and having them all in hand at the same time, that one could not view them, could not process them, together? What was the intent of that safeguard?

THOMAS RICKERT: Basically, this is language to ensure that nobody gets the expectation that they get full database access. So, as with other types of WHOIS that we see today, you issue one request, you get one return. No wild card requests [inaudible] to see what domain names or registrations might be behind that. That's to be prevented with this language. I don't see an issue with let's say a legal department of a company having identified ten strings or ten domain names that infringe upon their rights, to put them all in a box and get individual returns for those queries. I mean, that's a technical matter that you can submit those one at a time but technically those would be processed as individual requests. This is not about the implementation or display but this is just to confirm that we're talking about sequential requests for individual strings that produce individual responses. Does that answer the question?

MARK SVANCAREK: Actually, no. Well, it answered half of the question because it's that word "viewed". So, each string is individually requested. I can request an appropriate number of them in sequence and then once they are in hand, can I view them at the same time? Because there's this word "view" that I'm hanging up on.

THOMAS RICKERT: Okay. I don't have an issue with how it's being visualized. I tried to explain the rationale behind it. Let's find the right set of words to clarify that. And I have a point of order, actually. I've asked staff whether there's any chance we can see the notes, because I think as we move on, it's extremely difficult for us to take stock on individual points and just nail them down so that we don't have to walk back to them. For that, it would be beneficial to see what conclusions you've noted to ask for objections from the team.

MARIKA KONINGS: So, we're doing two things. Caitlin is taking general notes like we do for every meeting and I'm, at the same time, trying to make changes to the template based on the discussions here. Of course those are all going to be viewed, and where there's no agreement I'll put notes in there to make clear that what someone has suggested but was not necessarily agreement on that change. In

this case, for example, I've just added a footnote that explains a bit what this language means and it is not intended to limit the number of requests that can be made.

The challenge is if I share this as a Google Doc, you actually cannot see the redlines. So, I'm not sure how valuable sharing is. So, my idea was keep up and then, during the lunch break – or the working lunch – then be able to send out an updated version so you can all see it, and of course you can as well compare it with the notes to make sure that we didn't leave anything out. If you have a better suggestion of how we can do it …

Another option is I start sharing my screen and then you can see, but you don't see the original template. So, that's another alternative. I can start sharing what I'm doing here, so you can see that.

RAFIK DAMMAK: Okay. Thanks, Marika. So, we are already taking notes and we need also to check when we have agreement, so to be clear about that. So, if you can share your screen on the document you are working on, then I would ask everyone also to have the template on their screen so they can double check. So, if there is no objection, we can go with that and Marika can start sharing her screen. Okay.

So, next is Margie and then Thomas. Margie?

MARGIE MILAM: Can we see the … I'm trying to look at the language. I got lost. I think it's a little too specific on some of the safeguards. One of the concepts that we're interested in is being able to do correlation in order to support claims. For example, for a UDRP or a trademark infringement case, you can bring a case against someone who has multiple domain names. I'm not sure what the reasoning is to limit the kind of searching that can be done, assuming that it's technologically possible.

RAFIK DAMMAK: Thanks, Margie. Next, Alan Woods.

ALAN WOODS: On that point, Margie, and of course to what Brian is saying as well, I'm just going to blunt here in saying that what we're trying to avoid here is fishing expeditions. This is not the place for people to find the cases that they're going to follow. I'll give an example of being a registry, I get a number of – and I always like to remind people that the number is not huge. I think about 90 requests in the last year. But from those requests, a lot of them as specific – yes, trademark term but it is generic and it is in the midst of other words, specifically. It's very generic and it's very

specifically a difficult thing for me. As a registry, if I was to apply 61F balancing test, well this is [inaudible] trademark case and I think the suggestion is that the more of these I get the stronger my case is. That puts me on edge slightly. So, again, it's just that phishing expedition aspect of it that we need to be very clear in the safeguards and that should be another reason for [inaudible], that if one person or user is engaged in fishing expedition, then that could be a reason for [inaudible] as well. Again, bringing the safeguard. But this is getting to the pointy, blurry detail of how would we create such a review. But it is something that would be a consideration.

RAFIK DAMMAK: Okay. Thanks, Alan. Next is Alan Greenberg.

ALAN GREENBERG: Thank you very much. I fully support these shouldn't be fishing expeditions and wild cards should not be allowed as wild cards. We may well have a case where Facebook.X, that someone has registered every X in the syntax. But I really don't want to see restrictions in our policy on the implementation.

Now, just like ICANN compliance built a bulk submission tool, and if a registry or registrar has the capability of a bulk response tool, it shouldn't be precluded. So, our words shouldn't say "but you

must have singular responses coming back." That's an implementation. The requests all have to be valid according to the rules we're writing and that's the critical thing. We shouldn't be dictating implementation in our policy. Thank you.

RAFIK DAMMAK: Thanks, Alan. Brian?

BRIAN KING: Thanks, Rafik. I think we're zeroing in on language here for the domain-by-domain case. Sorry if it was misconstrued that we're looking for any kind of wild card in the domain-type request but I think we're getting there with the data has to be a domain-specific request. We're fully expecting that we will have a domain name and we will request the data for that domain name and then the data would be returned because we asked about a specific domain name.

Again, don't see any value in limiting it, if we have 10,000 domain names to send 10,000 requests. We have clients that have 100,000 domain names that are infringing that we are watching at a time. I don't know if contracted parties or whoever is going to run this system wants 10,000 different requests with one domain in each or if they want one request that has X number of domains in it where the representations that the requestor makes certainly

apply to all the domain names and they're specific to each domain name. I just don't …

So, however we want to make that work I think is fine but it would just be inappropriate to limit requests I think to just one domain name at a time full stop.

RAFIK DAMMAK: Okay. Thanks, Brian. So, for the queue, we have Georgios, then Greg, Milton, and Margie.

GEORGIOS TSELENTIS: Yes, thanks. Georgios Tselentis for the GAC. I would like to say in this discussion about the general safeguards that maybe we should see this from a point of view of what are the individual rights of the registrant, and therefore we should see the safeguards from this angle. Individuals should have the right to obtain on request, for example, a confirmation whether processing of their personal data relating to them and their communication is happening. So, I think this is inside the GDPR. They should have the right also to obtain a rectification in the case they have inaccurate data that are being processed. There should be, for example, not to be subject the individuals that if there is an automated processing taking place, that unless this is authorized by a law which allows that and provides, at this point,

appropriate safeguards, they should be able to also lodge complaints and also there should be to supervising authority and they should also be able to get remedies in front of a tribunal if these rights are violated.

So, I think the way we have structured the safeguards there, they should be seen from the individual rights of the registrant, as we are talking about the GDPR. However, we have to see also that the exercise of these rights can be restricted, can have reasonable restrictions, taking to account the legitimate interests of the individual. And at the same time, we should protect the rights, the freedoms, of others. So, it's in a sort of balancing exercise also regarding the safeguards.

For example, also, all these rights that I described should not obstruct official or legal inquiries, investigations, or proceedings.

I'm not so sure the way we have structured here the safeguards we can defer and we can defend primarily the individual rights, as we are talking about the GDPR and we can clearly put those caveats when those rights need to be exercised how this would be done.

I understand that this is we are at the start of this exercise but I think it needs a little bit more analysis in order to be reflected. Thanks.

RAFIK DAMMAK: Okay. Thanks, Georgios. Since I think you listed several items and got to elaborate them, can you please submit them in the chat so it's easier for us to capture and probably for everyone maybe to check them later, so we can also to include them in the document? Next is Greg.

GREG AARON: So, the bottom bullet point where we say viewed, we want to avoid that language I think because it implies that you can only possess one response at a time. I think what we're after is you make a request for a domain, you get a single response for the domain. Is that what we're after? So, maybe using that wording would be better.

By the way, that's the way RDAP generally works. You make a query, it gives you a single response. So, it might be technically correct as well. Then, Marika, can you scroll down please? Okay.

So, about volume limitations and slowed-down response times an CAPTCHAs. I think the first principle is: is the request a legitimate one? And if one has more than one legitimate request, one should be able to make those. And in some cases, users will need to make multiple requests because they have a good reason. If suddenly 100 variations of Microsoft show up in zone

file, Microsoft may need to understand who registered those if it wasn't them. And then they need to make those – they could make those in rapid succession and then they'll see who made those, and for example, find out if it's the same cyber squatter doing all 100.

So, volume limitations cannot be automatically imposed I think if there's a legitimate reason that each request was made, and I can maybe supply some suggested language here.

CAPTCHAs is not applicable because CAPTCHAs are for web-based lookups, and generally we're talking about a system and use of RDAP and similar technologies. Thanks.

RAFIK DAMMAK: Thanks, Greg. Next is Milton.

MILTON MUELLER: Yes. So, I wanted to emphasize that we do not see the safeguard regarding the individualized nature of the request as an implementation issue. This is a fundamental policy issue. It has to do with the nature of establishing legitimate interest. There can be no bulk requests, or as Thomas puts it, wild card requests. We would very strongly resist the idea that this is an implementation issue.

If Marika can pull back to … She had suggested some alternative language which I think says data for every individual domain name. It's moving around on us here. So, data for every individual domain. Hold still, Marika.

Yes. Must have a specific request submitted. Must, not much. That's closer to what we're getting at, I think. I think Thomas would agree. Again, it's meant to not so much rate limit – and I think Greg is correct about that. If you indeed do have 10,000 legitimate requests, you can make them. I don't think we can establish any kind of arbitrary limit on a number of legitimate requests. I think if people are somehow automating or abusing the RDAP in a way that has created a script that's running and simply …

But that was the old WHOIS where the data was just there and you could just go through it. Now it's based on an individual request that has to be essentially verified. So, I think we need to change the language about the rate limiting or the volume limitations as well.

RAFIK DAMMAK: Yes, Marika?

MARIKA KONINGS: I think I've seen several people supporting the alternative language. Is that something we remove that first part and kind of leave that for now and maybe move on front that point? Because it seems that people are agreeing. Is there any concern about that?

RAFIK DAMMAK: I guess we have agreement. I don't see anyone objecting. So let's make that change. Sorry?

ALAN GREENBERG: We have people in the queue who may be objecting.

RAFIK DAMMAK: Okay. So, let me check. Next is Margie, Hadia, then Alex.

MARGIE MILAM: Sorry, I don't know what we were voting on a second ago. Not voting but discussing, sorry. I'm confused.

One thing I wanted to point out that, even in today's system, some registrars actually want submissions of multiple domains rather than have them individual. We've kind of tried it both ways and some prefer it in one place, so that's why I want to stay away from as much implementation details as possible because I think

that's something that we can do on the implementation side and just keep the policy at a very high level. Thank you.

RAFIK DAMMAK: Thanks, Margie. Hadia?

HADIA ELMINIAWI: So, to Georgios' comment with regards to data subject rights and the need to include them in the safeguards, and also to Kristina's point where she was mentioning the need to make sure that the data is actually requested to be used and not compiled for other reasons.

I think having an auditing plan could be the solution to that. So, maybe we could add to the safeguards the need to have an auditing plan or creating an auditing plan. And the auditing plan definitely will take into consideration the data subject rights because it's an auditing plan mainly to ensure compliance.

I would also take into consideration what Kristina was talking about where she could actually make sure that the data was requested for usage through the auditing plan. Thank you.

RAFIK DAMMAK: Thanks, Hadia. Next is Alex.

ALEX DEACON: Thanks. I wanted to go back to our previous discussion. I noticed there's a bullet on the next … Oh, here it is. Accredited parties are not provided with bulk access. I'm wondering if this is not repetitive and perhaps we could combine with the previous bullet that indicates how data should be requested and what response will be returned. It seems to be repetitive to me. I don't know whether we delete that bulk access bullet or we somehow … If the term bulk access is somehow magic that we somehow merge it into the bullet above. But I think I would suggest we delete that bulk access bullet with the understanding that it's not even possible in this [inaudible]. Thanks.

RAFIK DAMMAK: Thanks, Alex. So, we have a proposal here. Next is Alan Woods.

ALAN WOODS: Thank you. I hope I'm not shot for suggesting this but maybe, Thomas, you might disagree or agree with me on this one. It goes back to Georgios' point which is absolutely a very good point in that we need to be clear on what those general safeguards are relating to. Are they relating to author or are they relating to the actual registrant themselves?

So, my tentative suggestion might be, to make this even more complicated, is to break up the general safeguards into

safeguards that relate to 51F which is the operational technical safeguards – I can't even think of the wording. You'd think I'd know this off my heart by now. One second, pardon me. Yes. The appropriate technical organizational measures. So, safeguards relating to that, that therefore they are the measures we are taking to prevent a breach. But then also break it down as to those that would be for the benefit of – those safeguards for the benefit of protecting the individual registrant or the balancing test in effect when we're looking at this one in a 61F. It would be those safeguards specifically that are the balancing test or in favor of or against the balancing test.

Obviously, it's not a perfect delineation but if we could come up with something that maybe just is a bit more sign-posty.

RAFIK DAMMAK: Okay. Thanks, Alan. Can you list those and send them to the chat, maybe? For you to double check. Okay. So, next is Thomas.

THOMAS RICKERT: It's nice that we speak after each other in this queue. I guess the question for our group to answer is to what level we want to include every single bit that GDPR requires for everything, i.e. general GDPR compliance in this document. I have intentionally not done so.

Once we start this process, we need to do the full enchilada of information to the data subject anyway, according to Article 13. We need to establish a record of processing activities. We need to talk about who is the controller and have the appropriate agreements in the background. So, I wouldn't put all that general points, including Georgios correct point in there. We can maybe say that we need to make this GDPR compliant in general and that would include the duty to inform the data subject about the rights they can exercise. So, I took that for granted. I just wanted to mention the points here that are specific to this very project.

One quick response to Aaron. Correct. I'm sorry. We know each other for ten years or so, so I don't know why that happened. With respect to CAPTCHAs. If you use RDAP only, that's fine but I would have thought that for certain types of implementations, there might be web-based access, and in that case, CAPTCHAs might be handy. So, I think the general notion is that we won't prevent any third-party, any rogue player from trying to reverse engineering the database with non-public registration data. And how we achieve that with response time limitations with a number of query limitations or otherwise, I don't that much care. We can leave that for implementation.

RAFIK DAMMAK: Thanks, Thomas. If I may ask here what you are suggesting is to think more about the kind of requirement to avoid that but not suggesting specific implementation. Okay. Next is James and then Mark. James?

JAMES BLADEL: Thanks. I just wanted to weigh in on this particular point with a question. So, my understanding is that the system we are trying to architect here is intended to cover, let's say, 90-95% of the most routine types of use cases for access to RDS. And there will always be other types of access. For example, we would respond to court orders and warrants and subpoenas and things like that.

It seems like what we're trying to do is to capture a use case that perhaps belongs outside of the system. I think that if there's a situation where someone needs to look up tens of thousands or perhaps hundreds of thousands of records that it might be more expeditious, instead of trying to bake that into the design of this thing, that we instead encourage those parties to work directly with individual registries and registrars because it seems like those would be more of an edge case.

I'm concerned that if we try to capture everything in one system, we're going to be here until the heat death of the universe trying to figure out how to make this thing bullet point for every possible idea.

And I just wanted to point out that this is not the only exclusive way to get this data. This is for the most common, the most frequent, the most routine and if you're getting outside of that, to Greg, to some of the use cases you described, then maybe this isn't the doorway you should be using.

GREG AARON: In the cases I described, this is exactly the system you would be using, [inaudible] for automated lookups.

RAFIK DAMMAK: Okay. Thanks, Greg. I'm not sure, James, if you want to respond. Okay. So, next is Mark and then Alan Greenberg.

MARK SVANCAREK: So, I actually got in the queue a long time ago but James has brought me back, so nice set up. So, regarding whether things are implementation details or policy issues, I did want to point out that I was talking to James offline and I've been working through our backlog and I would like to request from GoDaddy the many thousands of records of legal persons that we've been trying to use. So, I was just looking at our historical requests and there was a large number of legal person records or seeming legal person records that I would like to get reviewed.

In the current state of implementation, since RDAP is not available, I can't make several thousand one-off requests. It would be nice if I could say let's work together and figure out how to do this as a bulk thing. Now, this is a unique case but I wouldn't want to appear to be in violation of the policy that we're building right up in front. I think that there maybe some cases where that was in fact an implementation detail rather than a policy detail.

RAFIK DAMMAK: Okay. Thanks, Mark. Next is Alan Greenberg.

ALAN GREENBERG: Thank you. First of all, it wasn't clear to me that we're building the access system here as opposed to building a policy. Although James is right, we may want to handle some requests outside of the access system, I thought the policy we're discussing here applies to everything. So, I think we need to be very careful which we're talking about. Maybe we need to have clarity at which we're talking about.

In terms, again, of the bulk access – and when I say bulk access, it does not mean I want the whole database. It does not mean I want a wild card. But I may have a need for 1,000.

Now, if the bulk of the requests – excuse me, bad word. If the largest part of the requests are all identical and the rational is

identical and the legal basis is identical and the only difference is the spelling of the particular domain name, why would we want a contracted party to receive multiple copies, have to hold them up to the light to see if they're the same or not, whereas we could simply say all of this is the same, do the sanity check and the balancing once and then you can process the data? I would've thought that's an expediency issue.

And whether we implemented that away or not is moot at this point. I don't think the policy should forbid it. Thank you.

RAFIK DAMMAK: Thanks, Alan. Amr, please go ahead.

AMR ELSADR: Thanks. On the bullet for bulk access, as well as the bullet that was deleted on a single domain name – that only data of a single domain name can be viewed at the same time, the bullet we have here on the screen to me does not replicate the purposes of the other ones because one bullet addresses how a disclosure request must be submitted and then the others describe how a positive response to a disclosure request should look like. So, I don't see them cancelling each other out and I'm not sure why others think that it …

Okay. So, we have here the bullet that was deleted was only data of a single domain can be viewed at the same time. This was deleted or replaced by data for every individual domain name must have a specific request submitted. This is the first step, submitting the request. And this is the safeguard that describes how the disclosure request is submitted. The bullet that was deleted concerns the positive response to this data disclosure request. It describes a different safeguard to me. The same applies to the one on bulk access. I don't see them being repetitive or one making the other redundant. I'm still not coming across.

Okay. So, there's a data disclosure request. One of the safeguards on how to perform the request is that a disclosure request for a single domain name has to be done for this one domain name. The safeguards for a positive response to this request were a data controller or processor says, okay, we're granting disclosure to the data concerning this domain name. The second bullet addresses how this is done. So, one concerns the actual request, the other concerns the response to the request. They're not the same thing. Still?

[MARK SVANCAREK]: Sorry if I'm being slow. So, the reason that the bullet felt like it was redundant was that we were saying … I must ask for the data.

So, I ask for one name. I get the data back for one name. I don't say give me a wild card set or everything based on an entity or anything like that. It's simply request a name, support the request for the name with the appropriate [inaudible] and then receive the data back for [inaudible]. It felt to me like that handled both ends of the thing. So, how do you request it and then what is to be returned?

The line about viewing seemed to be a statement of here is a restriction on the subsequent processing that can be done, so that felt like that was a completely orthogonal thing to the requesting and disclosing and completely different again from the issue of bulk access, which I felt was covered by the requesting and the disclosing. So, that's where my confusion comes from. Did that make sense?

AMR ELSADR: Yes, it does. But part of what you're describing is now missing because it was deleted. Asking for the data for one domain name is there now but the part about getting the data only for that one domain name is not. That was deleted.

[MARK SVANCAREK]: But only the data requested can be supplied. See, that's where I feel like it's still covered. So, I can only request one thing and that

one thing only will be the thing that is supplied. It felt like that covered both ends of the transaction.

AMR ELSADR: To me, this might involve specific data fields on the domain name, so if you're requesting specific fields in the domain name on this one domain name, this bullet says that only these data fields are disclosed. But it doesn't specify to me that this concerns only one domain name. Does that make sense?

So, let's assume, for example, a data disclosure request is only requesting an email address. That's covered by this bullet but it does not necessarily specify data requests across multiple domain names.

[MARK SVANCAREK]: Okay. But that isn't a possibility based on the previous bullet. Do you have suggested language here that would resolve this ambiguity?

AMR ELSADR: Yeah. I just think that the bullet that was deleted should be [inaudible.

[MARK SVANCAREK]: Okay, which was the bullet that was deleted?

AMR ELSADR: Which was only data of a single domain name can be viewed at the same time.

[MARK SVANCAREK]: Okay. Well, it was the word "viewed" that was the problem.

AMR ELSADR: We can work around that word.

UNIDENTIFIED MALE: Well, he's asking for some of the language to be put back, so I'm just wondering … But I don't want to put that whole bullet back because there was a problem with that entire bullet. It was the word "viewed" which is the—

AMR ELSADR: Change viewed to disclosed, perhaps?

UNIDENTIFIED MALE: How about only the data requested … I don't know. Could you maybe suggest some text in the chat so we could move on from this?

UNIDENTIFIED MALE: How about if we replace the word viewed with disclosed? Only data of a single domain can be disclosed at the same time?

RAFIK DAMMAK: Sorry. I know it's becoming kind of … It's helpful back and forth but maybe just to take time and think about some suggestion and share it in the chat and we can come back because also we have people in the queue and I just want to listen to them. But we can come back to this discussion later on. Take your time and maybe discuss directly. Next is Milton and then Margie.

MILTON MUELLER: Yes. The delegate form Georgia yields the floor to the delegate from Canada because she could not put her hand up.

STEPHANIE PERRIN: Thank you, delegate from Georgia. I was waving, having my flag up, but I'm having real problems with Zoom, getting back into the stupid list of participants.

I just raised Milton's hand ages ago to clarify something that I think is being kind of merged and conflated, and that is procedures and safeguards. I mean, procedures are procedures. Safeguards are something that fit under procedures. You need procedures for the safeguards. You could look at it at both ends

of the spectrum. But management practices are not the same as safeguards and I think we should make this distinction fairly clear because the way you organize your management practices and procedures, you need to have some for safeguards and some for, in particular, transparency to the user about their user access rights and their right to be forgotten, etc. That was the only reason that I pestered Milton. Thank you.

RAFIK DAMMAK: Okay. Thanks, Stephanie. I guess next is Margie, then Marc Anderson. Margie?

MARGIE MILAM: So, the notion of showing one response per domain name, again it's way too detailed. If we've agreed that you could have a situation where there's multiple domain names that you have legitimate interest in, why do we care that it's displayed in [inaudible]. Why couldn't it be an Excel spreadsheet? As long as you've got the purpose and you've been properly accredited and it's a legitimate request. I think we're just getting way too granular here. I think the policy needs to go up at a higher level. That's something I think we should talk about. Then if you could scroll up to some of the points up there. Oh, maybe it's down. Sorry, go down.

The proof statement bullet I would replace with representations regarding use or non-use of data and appropriate auditing. Something to that affect, so that it's auditable. That's the way I would deal with that bullet. Thank you

RAFIK DAMMAK: Thank you, Margie. Marc?

MARC ANDERSON: Thanks, Rafik. I raised my hand because I'm concerned that we've gotten bogged down in the mud a little bit here. And judging by the reaction I just got, that might be a true statement. We also sort of have fallen into a trap of group editing on the fly, something we fell into in phase on a couple of times. I think we learned that that doesn't work really well for us. So, just a thought or suggestion. I think this is an important topic and we're on the right track here but this might be something best left to a smaller group or sub-team to take a deeper dive in and propose more fulsome language to take back to the full group. I think we're bogged down right now.

RAFIK DAMMAK: Thanks, Marc. Point taken. I think we tried to get input but there is no longer that temptation that we try to do some wordsmithing and so on. I guess we'll take input but to not get into the

wordsmithing and so on. I guess you want to add something, Marika?

MARIKA KONINGS: That was one of the reasons why we originally didn't put a redline up on the screen because it's very tempting then to focus on words and sometimes lead the way. Staff takes notes. They may kind of evolve based on the conversations. I think Marc's suggestions are really helpful, to keep it at a higher level and then either staff can indeed keep track of those suggestions and see how to reconcile them and come back either with proposed language or a small team does that. Either way is fine.

One of the open questions we still have and have not addressed is this notion of, indeed, is this supposed to include also the general safeguards that will apply to everyone and everything or is the focus going to be very specifically on this use case and what needs to be in place? I think Alan made a specific suggestion – that Alan, yeah – about maybe having two types of categories. That may be also a useful conversation to have. It will provide some guidance on maybe how to restructure this section based on your input.

RAFIK DAMMAK: Okay. Thanks, Marika. So, as you said, we try to avoid this kind of redline approach. But taking into account what was suggested for this subteam, I guess maybe we can try in the afternoon session to have a subteam. Maybe it's pretty much [inaudible]. I'm just checking here if it's a [inaudible] we can follow. Okay. If there is no support, we can have it later but probably we need before to get an updated version based on what we have as input and see later how we'll continue. Sorry, Hadia, for keeping you waiting. I'm not sure about the order. It seems it changed lately. I thought it was Hadia and then now Brian. Please, go ahead. Hadia?

HADIA ELMINIAWI: I'm not sure about what Marika wrote, auditing of these safeguards. It's too specific. It's the need to have an auditing plan, a compliance auditing plan. I don't think we need to put "of these safeguards".

I would also note that the data subject rights include transparency about the algorithms used and that would include being able to explain how decisions were made with regards to their data.

Anyway, again, if we are looking about auditing and GDPR compliance, all of that would be taken into consideration. Thank you.

RAFIK DAMMAK: Okay. Thank you, Hadia. I'm not sure. I see Brian and Milton, but Brian, I think it's a new hand. Okay, please go ahead. But just for Milton, is it a new hand? Okay. Brian, please go ahead.

BRIAN KING: Thank you. I'm looking forward to moving onto some of these other safeguards, so let's go. I think, as a quick point – and I don't want to belabor this now because I think we could use some legal advice on this. Well, this bullet may be redundant about the search functions on data elements other than the domain name and reverse lookups. Those might be the same thing. And they might be legal, so I'd like to put a marker there for us to explore in those cases.

The main point I wanted to make now is the disclosure requests directed at the contracted party that holds the requested data. I'm not sure what it means that the requestor directed at the contracted party and I want to be careful here that we're not pre-supposing an outcome. I would submit to the EPDP team in general that the contracted parties, if they're endeavoring to diminish their liability here might do well to have someone else be processing these requests, if not storing the data or controllers and we can talk about all that.

I guess I would question why a safeguard is where the requests are directed and whether it makes sense to rethink that concept or help me understand better what the value of doing that is – spelling that out as a safeguard. It's not clear to me, but I think that's a can of worms that we need to open.

RAFIK DAMMAK: Please go ahead.

ALAN WOODS: Sorry, I had my exasperated face on. You can't see what it looks like when I'm on the calls. Can we probably properly draw a line in the sand on what you just said there, saying that you would think that the contracted parties would like to [inaudible] liability? That is never happening here, especially … Me, as a registry, I'm kind of sitting pretty. My registrar friends are probably already six foot under on that because they still collect the data. The data still comes from them. They are never going to be not liable in this situation. I don't think we should be talking about concept of indemnity because that's just saying we're going to give people a cushion. Well, that's the next step, I'm foreseeing what the response would be.

The next step here is we are liable. We cannot farm it out to another controller and say, "Well, the data is no longer with us.

It's nothing to do with us." We are allowing them to fulfill this purpose. Therefore, we are still part and parcel of that processing sphere, so we cannot say that we should be open to passing on the liability. It's just not legally possible.

RAFIK DAMMAK: Thanks, Alan, and thanks, Stephanie. Next is Milton and Hadia. Alan, do you want to intervene again or do you want to pass your … Okay. I'm not sure, Brian, I think it's a new hand. Milton, please go ahead.

MILTON MUELLER: Okay. So, I wanted to address the volume limitations bullet. I thought we had agreed that this was technically inappropriate, inapplicable to the new system. Did anybody dispute that? Greg spoke against it. I said it didn't make sense to me. If Greg and I agree, it's probably a good idea. I mean, what happened there? At least could staff make a note that there's some questions about the applicability of this concept of CAPTCHAs, volume limitations, slowed-down response times? That certainly made sense in the old WHOIS where the data was just there and you were vacuuming it. But I don't understand. Again, I'm opening to somebody explaining to me. I don't understand the relevance of that bullet. Maybe Thomas can explain what he meant by that.

THOMAS RICKERT: I can't help responding to Alan briefly. This is not the work for [vicarious] redemptions, unfortunately. To your point, Milton, I guess it's not unknown in the industry that registries, for example, have a maximum number of queries for the registrars that they're serving. So this is something that we're known to.

The reason for putting in safeguards in place is that we can't just build the system on trust by somebody making a statement up front that they will limit the queries to using the data for certain purposes. So we need to take precautions against rogue players trying to gain the system.

I think one way of doing that is building in technical safeguards. I think if somebody, as in Brian's case, I think it's perfectly thinkable that there is somebody who has identified tens of thousands of domain names that might infringe upon their rights. But the question is whether the default setting of that system should be that you can find as many disclosure requests as you want to. And I think probably the answer should be no, because if we have a breach scenario where somebody fooled the system and tried to reverse-engineer the entire concept, the authorities in a supervisory proceeding will ask us about our thinking about privacy by design. And I think it would be a design feature to have certain limitations.

That doesn't mean that for certain use cases the thresholds can be limited, can be put at a higher point at some point, but I think we need to think about these. The limitation can be 10,000.

MILTON MUELLER: Alright. I understand what you're getting at now and I think I support it then. But you understand that CAPTCHAs may not be technically appropriate form of limitation here.

THOMAS RICKERT: Brief follow-up. I tried to respond to the CAPTCHA thing when Greg brought it up earlier. When this was drafted – and actually, as I said during the last call – we put together these ideas when we drafted the GDPR domain industry playbook. We thought that we would have different routes to get into that non-public data, one of which would b web-based, one of which would be RDAP-based, for example, and for the web interface that let's say folks with small volumes of queries might use, they might go to a web interface and their CAPTCHAs might make sense. I'm happy to remove that. I'm just saying that we need to give some thought to design principles to honor the principle of privacy by default and privacy by design.

MILTON MUELLER: Why don't you try to reword it in those more general terms as a mechanism for avoiding gaming or abuse of the system?

THOMAS RICKERT: That's perfectly fine by me. The reason why I had originally raised my hand was the point that – I guess a policy point that should have been explained slightly more wordy. We have a de-centralized system at the moment where data is not sitting in one central database but it is in various places. I think that one of the – or that the system, at least at the moment, can't be structured so that you can go to any registrar and say, "I want you to get the data for domain that is sitting with a different operator." But the requestor should do some investigation and find out with what registrar, what ICANN-accredited registrar, the data is actually sitting and then go to that contracted party and ask there.

In the absence of a centralized system, RDAP can do that, but as long as we don't have a centralized access point, I think the onus should be on the requestor to only be able to approach the contracted party that actually holds the data. We can frame that point differently also, but that was the logic behind it.

RAFIK DAMMAK: Okay. Thanks, Thomas. So, just maybe time check here. At noon we will have our working lunch session with presentation. So, we

should have maybe five minutes before to get lunch and to not waste time. Also, we still have a queue here, so I want to close the queue and to give a chance for those who are there to speak. Next is Brian. Thomas, do you want to speak again? Okay. Then Greg and Alan. Brian, please go ahead.

BRIAN KING: Alan walked away. We should talk about that part of the conversation in the future, I think. I haven't heard any responses. I'd like to explore what we're safeguarding against and what that bullet even means about the disclosure request must be directed at the – insert X party here that controls the data. What's the problem that we're trying to address with the safeguard? Because it's not clear to me what this does.

THOMAS RICKERT: I can try to reframe the answer that I previously gave. At the moment, we technically don't have a centralized starting point for WHOIS query, for all contracted parties around the world. Therefore, in the absence of that centralized system, the idea was that the burden is on the requestor to find out what contracted party actually holds the data and that can be the registry, and more appropriately, the registrar that is supporting that particular domain name.

What I want to avoid with this language is that you can go to registrar A with the expectation that registrar A can get you the data that is with registrar Z.

BRIAN KING: Thank you, Thomas. RDAP actually does that with the bootstrapping mechanism that allows you to submit an RDAP query and follow the referral length from the registry to the registrar, the authoritative registrar, to pull that data. So, that's technically possible now – or August 26th when RDAP goes into effect. I guess is the risk here that we're implicating a different registrar who is not the sponsoring registrar for the domain name in some data-processing risk, I guess? Is that the concept?

THOMAS RICKERT: That was the idea but we can remove that. I mean, I'm just trying to explain the rationale. If the group thinks that we can remove the language, I will not fight for it.

RAFIK DAMMAK: Okay. Thanks, Thomas. Just to be clear, we still have a session in the afternoon we continue deliberation. As I said before, I can cut the queue. So, for Margie, I see you. When we come back … I mean, after the working lunch session, you will be the first in the

queue. Sorry for that. Let's go with Greg and then Alan. Greg, please go ahead.

GREG AARON: Our current use case is talking about intellectual property uses. When we talk about volume limitations and slowed-down response times, if we're talking about applying that elsewhere, it's going to be highly problematic, especially when we start talking about security uses which are very different. So I don't think this language may translate to some other use cases. And when we get to that discussion, we'll talk about SSAC 101 which was a paper about rate limiting. So this might be fine here but not in other cases. I'll leave it at that. Thanks.

RAFIK DAMMAK: Okay. Thanks, Greg. Alan Greenberg?

ALAN GREENBERG: Thank you. I'm on the same topic. When we last talked about this a few minutes ago, someone pointed out that we have to be careful about bad actors who may be making bulk requests in huge numbers and doing unreasonable things. I think we need to think about bad actors on the other side as well. We could end up having a registrar who decides that mass access is once per month, and effectively cut off all service based on what they

define as unreasonable. So I think we need protections on both sides, not just one side. Thank you.

RAFIK DAMMAK: Okay, thanks. We'll stop here and then we'll continue the discussion in the afternoon session. Marika, do we have any logistical information to share before reconvening at noon for the lunch session?

MARIKA KONINGS: Thanks, Rafik. We have a couple of guest speakers that will join us for lunch, so we'd like to encourage everyone to be back here at 12:00. So you have a few minutes to just run outside, go to the restroom, and then as soon as the boxed lunches arrive, we'll just distribute them so at least we don't interfere with the agenda. Or if they have arrived just before we started, you can of course pick them up yourselves. But that's the plan.

RAFIK DAMMAK: Thanks, Marika. Yes, let's be on time, just one hour for I think two presentations, so we need to …

MARIKA KONINGS: Just one more thing, that the order of the presentations will be reversed compared to what was on the agenda due to the availability of the speakers.

RAFIK DAMMAK: Okay, thanks. So, that's it for this session and we'll come back at noon sharp. So, thanks everyone.

UNIDENTIFIED FEMALE: The boxed lunches are over here for the EPDP team members if you could come over and make your way.

RAFIK DAMMAK: Okay. Thanks, everyone. I said we will start on time, so I ask EPDP members to take their lunchbox and take their seats so we can start. Giving you one minute to do so.

Okay, everyone. Please take your seat and let's start. Thanks.

So, for this session, we'll have two presentations. We have guests who proposed to present some of what they were working and trying to solve. We can maybe benefit from this presentation and see how we can help us for our work. We'll start first with this presentation about the curative access platform. It's from our guest, Bart, from PWC. Okay, Bart, please go ahead.

BART LIEBEN: Thank you, Rafik. Good afternoon, everyone. I hope you enjoy your lunch and I'm hoping that we're not going to heat up this session too much because it's quite cool in here. In any case, thank you for having us, Rafik and the EPDP team.

There are basically two parts to this presentation. I have a few slides to show, and if there's still time left, because I know that Mike is also eager to present, we're going to give you if you want a small demo of what we've been working on.

What we've been working on is basically a proactive solution. Some people in the room may remember that the first discussions on GDPR and compliance WHOIS were initiated back in 2016, actually during Marrakech I think it was 55, where we were looking into developing for specific TLDs a number of systems that could deal with controlled access to non-public domain registration data.

Our initial starting point of developing this system was April 2018, so before the ICANN specification has been published. We were looking into this not only from a GDPR perspective but also from a more global perspective. GDPR is, of course, a very important new framework that has to be taken into account, but if you look at countries like Singapore, they were already there in 2012. We see a number of other countries developing new legal frameworks, like Brazil that just implemented something and

China is definitely working on something that is much stronger to a large extent than what GDPR says.

So, GDPR is just one of the inputs for us. We've been looking at this from a much more global perspective.

We've also recognized in doing so the compliance burden and the risk sentiments that we apparently have with contracted parties, so we are trying to come up with solutions to mitigate those concerns.

We've been working four different [trunks]. First of all, making a technology framework that is modular, versatile, scalable and that actually works. So, that's one. Compliant not only with GDPR but also with other data protection laws across the globe and keeping with the PWC global network, keeping close track of whatever is happening there.

We're looking at a technology neutral solution, so that's one. And secondly, also, cross-neutral solution for contracted parties. So, this is more or less the framework that we're trying to design.

To give you a bit of an overview, as I mentioned, we started in April 2018. Quite a few people in the room have been interacting with us or we've engaged with them in order to see where can this lead towards. Of course, we've been following up closely the work that has been done by the EPDP.

Our next steps are interacting with you, so definitely with the EPDP group but also with other people who are interested because, ultimately, it needs to be that solution. That is a [inaudible] versatile, scalable that works that is fully compliant. So, definitely testing is a critical element in that respect. So, if you have ideas or if you want to join us in performing a number of testing activities, please do reach out. Our idea is to have a [goal life] as what we refer to as our MVP 2.0 in Q3 or the beginning of Q4 of this year. That's the objective that we've put forward for ourselves.

We're basically looking into two different steps, which are probably not new, definitely not for the EPDP team. So, identification of the requestor and determining the capacity in which the requestor is acting. We want to provide assurance – that's what PWC stands for. We want to provide assurance that requests are logged and data is provided to parties who claim, who appear to be what they claim to be or who they claim to be and that these are going into a very specific category of users. So, we're talking about law enforcement agencies, we're talking about IP owners, we're talking about security experts. At this point in time, it's an undefined list of or unfinalized list of potential requestors, so also there any input that you may have or suggestions that you could have, they're definitely welcome.

So, verification of what they do that's based on agreed-upon procedures is something that PWC of course has been doing for quite a substantial amount of years or number years. So, it's looking at, well, whatever works within a specific country. You have countries where nothing where you don't have ID cards, for instance, so you need to find for alternatives. So, what we've done throughout the network, we've established a baseline set of criteria against which potential requestors can be vetted.

Authorization. One of the points that I think were mentioned by Milton this morning was how do you do that? Is that on an individual level or at the organization level? There are definitely ways on how you can do that at the organizational level that you have, for instance, the FBI is saying, "Look, we are accredited and these are the users that can use the system." So that's something that we can put in place. We do not necessarily have to put it in place. We're following up the policy development process that is currently ongoing. But these are definitely features that have already been incorporated in our demo platform.

Initially, we see this as a one-off process, possibly with regular confirmations. So, any registrant of a domain name in gTLD gets an annual confirmation email, so we're looking at something which is similar to that process that already exists.

Step number two. So, we now established who can access the platform, who has provided for necessary guarantees, who has agreed upon terms and conditions, what they can do with the data, how they should log the information and so on – that whole framework of processes and legal terms that have been passed. At that point in time, we can start receiving, processing, and fulfilling requests.

As I mentioned here, it's initiated by authenticated users who must include and indicate for which purposes that they are going to need access to non-public domain name registration data.

What we have done, because we started slightly ahead of EPDP becoming established and the process that is currently still ongoing, we have been looking at about 40+ pre-defined scenarios where a type of requestor acting in a certain capacity wants to have access to certain data in accordance with certain justification that they want to put up.

So, what we have done, as I mentioned, we are looking at this from a global scale. We have developed those templates initially as being GDPR compliant as vetted by GDPR privacy, data protection experts within PWC Europe. And we sent out across all the different PWC countries in order to get a local approval, comments, inputs, and so on.

So, that resulted in those 40-plus pre-defined scenarios which we have included in our platform and will show you in a few minutes how that basically works.

We've aimed here to maximize a number of scenarios. So, to minimize manual processing. So, the ideal situations that as little as manual intervention is required in order to log a request, obtain the data of a specific registrant which is not in the public domain.

Also, requests are submitted to registry and registrar and fulfilled in real-time. So, we don't need full access to everything. We're not storing copies of whatever databases that there are. So, everything is going to be fulfilled in our proposed model in a real-time context.

So, then very important of course is how to ensure that this all is complaint. What we have done that's also in the demo which we can show you later on is we've developed an initial baseline framework. This has been described into templates, so we have about 40-plus templates currently available.

We, of course, have been looking at the tremendous amount of work that the EPDP group has been doing. Basically, it's an open invitation to work together in order to see how we can take that one step further. So, we're not definitely in the policy development sphere. We jumped the gun a little bit. We made a

little bit of a head start from the beginning of summer last year in order to see where in terms of functionality the system could evolve towards.

So, we must be however realistic and pragmatic. That's definitely the lesson that we took from consulting the different PWC countries. So, first of all, as I mentioned before, these laws, these guidelines, these processes are in constant flux. It is something where basically there's an ongoing policy development process necessary in order to keep abreast of all of those changes that are currently taking place. GDPR has moved the post quite a bit and we do see that countries are catching up. So, it's not only GDPR. It's definitely something that needs to be looked at at a global scale.

We also see that it's difficult to get some kind of an [inaudible] pre-approval from official organizations, like data protection authorities. So, to a certain extent, there is a risk element still involved, so we can't deny that being there.

We've also taken into account the fact that contracted parties will remain cautious and seek additional assurance, bearing in mind their own specific scenario, their own specific situation, their own specific interests. So, we have factored that element in. We're not saying that it must be something that you as a group must adopt. We have included a number of options that probably will be

discarded when we're going further into that process or which need to be added later on. So, we have looked at different possibilities in that respect.

Very briefly, how does it work? You have a requestor. You have a registry, you have a registrar. Requestor is being authenticated against these pre-approved procedures, as I mentioned. And there is a specific module that we've developed for handling those requests and complaints with respect to domain name registration data that is not in the public domain.

Underneath, there is a rule engine that we've developed, which includes those, as I mentioned, scenario templates which takes then care of the data processing.

Initially, in our [MVP] 1, and we're not saying that it must be the ultimate solution that we're proposing because you'll see that there are also different options in place for you as a group to consider, if you want to go down that path. We are seeing this as being within the PWC environment. There are a number of reason for doing that. The main reason being that we can, at that point in time, provide for end-to-end assurance. Contracted parties want to be assured that the data that is being processed is done in a complaint way. If you keep that within a controlled environment, that's something where an organization like ours can provide the necessary assurance.

As I mentioned, the way how it works currently, we can make available the baseline templates that PWC has developed at an international scale. And then it's up to the registries and registrars absent any final policy decision at this point to say we feel comfortable with those scenarios and those templates, or we're not feeling comfortable. And not feeling comfortable can be for different reasons.

You may be a corporate registrar that says, "We only have corporates. We only have organizations. We do not process any personal data in the non-public domain name registration data that we're holding from our customers, so we want everything to be on the open." So, that's perfectly possible within this model because you, as a registrar then, as a corporate registrar, can basically say, "For any request that comes in from anyone, you just present everything," because definitely for quite a few brand owners or government institutions, for instance, there's a vested interested in showing to the world that you are who you claim to be.

In other situations, you may have a registrar or a registry in a certain country that says, "Well, we have obtained guidance from our local DPA and we think that the actual structure and the contents of whatever is being provided as a report ultimately needs to look differently." So you can switch off a number of data fields, depending on which scenario that you're choosing.

So, whenever the requestor starts requesting data on the platform, we have authenticated the requestor, checks for data access permission. At that point in time, registry database, registrar database has been consulted. Data is being delivered to the system. The rules that have been set by the policy development process and/or the registrar and/ or the registry are being applied and the report is being delivered to the requestor. It's basically a rather simple process as from that point.

A very important element into this discussion is of course about responsibility and accountability. As I mentioned, if you centralize everything, it has a few upsides, it has a few downsides. We are quite open on that.

Here in the proposed model, on [MVP] 1, is that the authentication process and the authentication itself is being managed centrally. As you will see in [MVP] 2, we're taking that one step further. We're having baseline scenarios in place for request processing and fulfillment, which in our view, are complaint with applicable data protection laws but which also provides us with the possibility of making swift changes if needed be.

I'll give you one example. If you look at all the registries and registrars that are out there, including reseller, including ccTLDs, you're talking about quite a few thousand potential interested

parties who are part of this. If a data protection authority from a certain country at some point says, “In this particular situation, you can’t provide this or that particular piece of data,” if it’s not centrally managed, that means that all those thousand parties need to do interventions themselves. Being compliant with a scenario where the data protection authority has taken a decision upon.

If you manage it centrally, it takes literally two minutes to implement that decision from the relevant data protection authority and all the parties who are connected to the system will be compliant as from the get-go.

So, that is one of the benefits that we see of the centralized managed system. There are of course a few downsides but these are definitely to be overcome. We’ve been in previous scenarios where also there was one party that was open to doing a number of things for the community and these also worked I think in the end.

So, this is also then the party that provides responses in line with the compliant templates, as determined by EPDP, the community, registry, registrar, you name them. And to a certain extent, if there would be a complaint later on, this is also where the operator of this model would be managing or participate in that complaint process.

Again, the idea of [MVP] 1, we see it is providing as providing end-to-end assurance and take responsibility for that process. So, it's very much the idea where we say to contracted parties, to a certain extent, you can outsource that compliance operation to that centralized party.

If we're looking at [MVP] 2, we're looking for having those modules that I mentioned before being spread out. It's an option. You may be a registry or registrar that says, look, we want to do that complaint handling, we want to do that request fulfillment process – we want to manage that ourselves. So, we want to have that module in place. We've built [MVP] 1 in a modular way so we can disconnect the different components here. And then of course make available templates whenever it needs to be, but at that point in time, of course, it's up to the party concerns to make sure that those templates are uploaded, that software is updated, and so on, so there's a bit more handling at the side of the contracted parties at that point.

So, currently, we're looking at the system where everything goes in [MVP] 1 as option one through one single entity, but it's possible here to have authentication being done by the centralized party, request logging and fulfillment being done by the registry itself. Take a registry here as an example. Or if you take it one step further, that for instance say you have one single or even multiple authentication servers, if you look at it from a bit

more federated approach, that could be spread out as well and where you have authentication requests, logging and fulfillment, being with a contracted party itself.

So, that's what I meant when I initially said it's a technology neutral operation. So it's perfectly possible to have a federated approach in terms of authentication, and to a very certain extent, also the request logging and fulfillment bit.

Just to finish my presentation, and I propose we go to the demo, what are we looking for? Well, again, thank you for inviting us to give that presentation. We're looking for input. So, we can give you a short demo now, but do reach out to us if you think you can help, if you have comments, if you want to make it better. There's definitely room for improvement. We're not saying that this is the only model that will be available. We're definitely looking for working with you in order to see how we can take that forward. We have been interacting with quite a few of you already and also thank you for taking that time. Basically, we're looking for, to a certain extent, a validation of the baseline system and developing an operational and business model later on. We can bring an [MVP] 2.0 to the community, let's say, September or somewhere around the Montreal meeting later this year.

That concludes my presentation. If you're still interested, we can quickly show you how part of our system works. We're looking

mainly at the requestor fulfillment and the receipt of the request and the processing of that information, so to get us online.

KRISTINA ROSETTE: Sorry to interrupt, but before we get too far into the demo, I suspect that a number of us have a lot of questions.

BART LIEBEN: Sure.

KRISTINA ROSETTE: And in fairness to the other presenter, I'd like to ensure that we have time to go through questions before we do the demo. Would that be all right?

BART LIEBEN: That's fine.

KRISTINA ROSETTE: Thank you.

BART LIEBEN: So, any questions then?

RAFIK DAMMAK: Okay. I'm not sure I see. I'm checking in Zoom and I see there are some queue. I think we have Ashley, Owen, and then Kristina. Actually, it's an old hand. So it will be Owen.

OWEN SMIGELSKI: I don't mean to question any altruistic methods here. I think a concern for the contracted parties is what's the funding method, are we locked in, is this some sort of patented proprietary system that can't be duplicated elsewhere? Is that a concern or is that something that we shouldn't really be too worried about?

BART LIEBEN: It's not a concern, no.

OWEN SMIGELSKI: I guess a follow-up, that means we don't have to worry about the funding, don't have to worry about any patents or anything like that?

BART LIEBEN: You don't have to worry about it, no.

RAFIK DAMMAK: Okay, thanks. So, we have Kristina and then Stephanie. Kristina? You can come back.

KRISTINA ROSETTE: Sorry, I'm good. Oh, yeah. Why don't we … There actually are a number of questions in the chat that precede my intervention, so let's go to those.

RAFIK DAMMAK: Okay. Sorry. The question … So, you mean from Volker. Usually, it should be one of the … I understand Volker is not here but it should be usually one of the representatives but we can read them for this time. We also have Stephanie in the queue.

So, first question is: how does PWC envision a balancing test to [inaudible] in a practical level if the process is non-manual? And the second: does this replace RDAP?

BEN LIEBEN: Second, no, it doesn't replace RDAP. The balancing test for the manual process is something that has to be established, so that's definitely where we're looking for policy development to see to which extent the operator can take certain steps whenever a request comes in. So, that's why we're saying that we're trying to maximize the number of scenarios that we can envision, so we can standardize that process. And if you can standardize a process, you can automate the process.

Hence, us reaching out to all of you to give us a many use cases as you can, so we can do that vetting beforehand and we only have to deal with the exceptions later on – because there will be exceptions. We've been through these processes before. We know that these exist. Then, it depends really on the outcome of the EPDP to see to which extent there is liberty or there is a level playing field for the operator to take determination or make determinations to interact with the requestor and so on and so on.

So, these processes, we've done those in the past, so it can be done, and of course definitely with PWC we have sufficient privacy experts in every country on staff to deal with those things. Yeah, that's definitely possible. Yes.

RAFIK DAMMAK: Thanks, Bart. I'm not sure, Kristina, you want to intervene?

KRISTINA ROSETTE: I'll go. Just following up in the interest of fairness, I will ask a modified version of a question that I posed to Steve Crocker when he presented to us. Obviously, PWC is funding this. Are there any other entities that are funding or will benefit financially from this?

The other question is: cost neutral doesn't mean free, necessarily, so I was hoping you could elaborate a little bit more on what cost neutral actually means for the contracted parties. Thank you.

BART LIEBEN: Well, at this point, at this moment, in all fairness, we do not have a really a finalized business model for this because we're lacking a few parameters. That includes, for instance, what are the number of requests? I think it was on my last slide. How many request are being submitted by whom? What's the nature? What's the extent? There's quite some information missing in order to come up with a proposal that says, look, this is the way how it's going to operate?

Hence, again, me reaching out to you and saying how many requests does the Federal Bureau of Investigations do on a daily basis or on a weekly or monthly basis? Are law enforcement agencies willing or able to pay for a service?

I think we need to have those baselines in place in order to come up with some kind of a model. But again, the outcome for us should be that it's technology neutral. So, we're thinking, for instance, of a way where you say there's a cost that is being incurred by stakeholders, by the contracted parties for instance, but where the requestor who lodges a request has a fee, pays a fee, per lookup where we're done offloading or taking the cost

that we've sent to the contracted parties, and to a certain extent, compensate with the income that you get from a per-request basis.

Does that mean that we're only looking on a per-request basis? No. Because again, we're lacking sufficient and reliable data in that respect. So, if someone from you could give us some idea on what, from your constituency or from your organization that you're representing how many requests that you're sending or receiving, it can help us in developing model and we can be extremely transparent about how that model looks like, so that's not a problem.

RAFIK DAMMAK: Thanks, Bart. We get the last question from Stephanie and then we can continue to wrap and move to the next presentation. Stephanie?

STEPHANIE PERRIN: Thanks very much. My first part of my question relates to transporter data flow. I wonder how you're handling it. Many countries have export of data provisions intact. Data commissioner in Canada recently suggested that individuals had the right to consent or not, which means even … It's not a federated system. It's a messy one, right? So, how are you

planning to manage that? And I'm well aware that most of these provisions aren't actually being enforced. Doesn't mean they won't in the future.

Second question. I'm the head of the Non-Commercial Stakeholders organization and I wonder if you've been working with us, and if so, with whom? And of course I'm dead curious to know who you have been working with and whether it's on a client basis. Thank you.

BART LIEBEN: So, to answer your question number one, we are aware of the fact that these things exist, so these laws exist for limiting the export of data and to which extent and so on. So, there I think, as an organization, we have access to the necessary authorities in Canada or in any other country in the world in order to see how we can find a solution that makes this offering compliant, not only with privacy laws but also with other laws that may exist. So, I think these contexts are there. We can definitely talk to you about it. Thank you for flagging the issue.

So, we're willing to offer or are proposing to offer a compliance solution that's not only looking at data protection, it's looking at the entire [thread].

Now, it's also not a solution that will bring world peace, so let's be clear about that. We're thinking about that in [MVP] 4. But that's not there yet.

With respect to your second question, I have to check to whom and whether we have reached out to your constituency, so I can't give you a clear answer to that at this point.

STEPHANIE PERRIN: Thanks. And with respect to the [TBDF] problem, it's really the constitutional protections that I'm concerned about, because the moment you take the data out, we have no constitutional protections anymore. Thanks.

BART LIEBEN: Yeah, absolutely. So, there are potentially ways on how we can go about that. Of course, PWC has offices in Canada, so there's a way probably how we can find some kind of an interim solution that could work. But I can't give you any full detail on how that is going to work at this point.

RAFIK DAMMAK: Thanks, Bart, for this presentation. I guess if there aren't any questions or input, maybe we can share them later or find how to – yes?

BART LIEBEN: I'm appreciative of the time and we definitely need Mike's 45 minutes as well. We do have a demo of this, so let me propose that if you would be interested, our contact details I think are in the presentation, so do reach out. If not here, we can do it definitely in a video conference to your constituency, to yourself; it doesn't matter. We're really seeking input and looking forward to working with you. Thank you.

RAFIK DAMMAK: Thanks, Bart. Just to finish here, you said you have over 40 scenarios. Is it possible to share them?

BART LIEBEN: We can definitely share them, yes.

RAFIK DAMMAK: Okay, thanks. Thank you.

BART LIEBEN: Thank you.

RAFIK DAMMAK: Okay. The next presentation is with Michael.

BRIAN BECKHAM: Good afternoon. Thank you, everyone, for the opportunity to present with you along side Michael Palage. Is that better? Okay, thank you.

For those of you who don't know, my name is Brian Beckham. I'm with WIPO, the World Intellectual Property Organization. And along with Michael Palage and Frank Cona with InfoNetworks, we'd like to present to you some thoughts on a potential solution to third-party access to non-public registrant information. If I could have the next slide, please.

So, many of you know WIPO through its work managing the UDRP. We're active in the rights protection mechanism policy discussions. But for those of you who don't know, this is just one of the services that we provide. We are actually a global inter-governmental organization that is the global forum for intellectual property services, policy, information, and cooperation. And what that means practically is that, if you will, there are two buckets of activity that WIPO manages. One is nor making and the other is the provision of services. So, if we could move to the next slide.

One of the areas where WIPO has been engaged in nor making was the creation of the UDRP, the Uniform Domain Name Dispute Resolution Policy, back in 1998 and 1999. And of course in terms

of the provision of services, we have been managing and running UDRP case administration services for the past 20 years. Next slide, please.

I think it's safe to say, especially with this audience, that current accuracy and access to WHOIS information has, throughout the history of the DNS, been an area of concern for different stakeholders for different reasons, and since the coming into force of the GDPR last May, this has been an area of increased attention.

One of the areas where we've been particularly interested from a UDRP service provider perspective is that we require certain registrant information in order to fulfill our due process obligations to registrants of domain names through the temporary specification and subsequent iterations. We've been able to obtain that information from registrars, but obviously it's an area where we have a strong interest in terms of being able to provide our service and provide sufficient due process for registrants to be able, in that UDRP provider role, to obtain WHOIS information. Next slide.

So, with this slide, I want to transition over to Michael and wanted to just say that we, since even before the GDPR's coming into force, have been approached as potentially playing a small role in the broader chain of a unified disclosure or access model. One

of those specifically being validating the existence of IP rights and authorization of an IP owner or an agent to try to participate in the access model. So, I want to be clear here that we see our role, if these policy discussions go in this way, as a very limited role, limited to the verification of the existence of an IP right, whether that's submitted on behalf of the rights owner themselves or through an agent. And this is just one small piece of the bigger puzzle.

So, with that, I'll turn it over to Michael Palage.

MICHAEL PALAGE: Thank you, Brian. Next slide. So, one of the questions – Kristina, I'll answer your question about interest and why we're here. InfoNetworks, the work we've been doing is self-funded and a lot of this is actually in connection with work that we've been doing with other verified TLDs. People in the community know that I've worked closely with dot-bank, dot-insurance, dot-coop, dot-sport, all registrant-verified TLDs.

The one specifically that was the genesis of the work that we're presenting here today is some of the work that I'm doing with the Universal Postal Union in connection with dot-post. So, this is something – and again, just to hit pause here and to go back to something that Steve Crocker told this group that he's presented. Steve said he's been dealing with this subject for two decades. I

myself can equally make that statement. In fact, it was at ICANN 3 in Santiago, Chile where some of the first issues of access and accuracy was first discussed.

So, part of what I think is a real opportunity here is we have the chance … The GDPR is probably a once in a lifetime chance to get something right. I've seen 20 years of putting Band-Aids on a problem. I think if we follow through with what the GDPR is about, privacy by design, we can get that done.

One of the things that I think is also important to mention in connection with the UPU and the postal operators is they actually have a global standard on identity management. It's S68. This is something that has been adopted by 192 member countries which are signatories to the postal treaties.

This is something that, as I said, as part of our pilot, we have already started actively interfacing with the open RDAP databases. We've actually interfaced with a number of registries, EPP systems. So, this is something where we are willing to work with people to show what can be done. Again, we'll get to that a little later on. Next slide.

So, let's talk about the criteria for success. One of the things that I think when the initial discussions between Brian and myself, WIPO, we wanted to talk about what was the framework. And as

Brian said early on, they acknowledge that they wanted to have a very small piece of this overall holistic solution.

One of the things that they did not want to be involved in was digital identity proofing. So, one of the things that is perhaps different in our approach here is on how we try to handle that identity solution. Instead of necessarily, in connection with Bart's PWC model where they are the verifier, we actually want to sit there and actually have that opened up to a free market where we potentially could leverage other identity systems, even national identity systems.

So, in connection with the EU, there's the eIDAS regulations that were passed last year. Those would be credentials that would be able to provide a basis. So again, that's one of the things that's important to look at.

Another approach, as I said, since the genesis of this project lies with the work we were doing with dot-post in the UPU, we need to account not only for the GDPR but those other countries that have even much more stringent, particularly those countries that are going down the route of data localization laws. So, this is something that has been very fundamental to our approach.

With regard to legitimate interest, one of the other aspects that we've looked at is while we're going to focus here today just on intellectual property as part of this joint presentation, we've

actually looked at some of the unique needs of cybersecurity researchers and national certs that do not necessarily need to get to the underlying PII data but potentially [inaudible] to do analysis. So that is something that also is incorporated into our approach.

The other question I believe that also came from the contracting parties house that I will address right now, the work that we've done, open standards, improving technologies. So, we're not doing anything that is proprietary. Again, when you work with UN agencies, that's something – their member states hold them accountable, so this is something that what we're looking to build upon.

We tried to sit there and make what we've done – or the proposed changes, we tried to go from a minimalist changes to the system to minimize the risk.

Regarding funding, we basically are going to make this, if you will, economically self-sufficient. And to that point, we will make this entirely user-driven. So, this is not a situation where we will be expecting to impose any fees on registries or registrars. That is our intent.

One of the other things that I think is interesting – and this is the point I was alluding to earlier about trying to foster competition and innovation. One of the interesting things about the UDPR

when we first were discussing that back in 1999, the original draft only called for only one UDRP provider. But what happens is the community discussed that and said if ICANN is about innovation and competition, there should be potentially multiple, equally accredited UDRP providers.

That's what we're trying to do here is we want to sit there and foster a growing, what we see industry of identity providers. There's been some excellent work, for example, done by DNIC with the [ID for Me] initiative which we think is interesting. A lot of European ccTLDs have already integrated digital identity into their domain name registration process, so the idea of moving digital identity and these other frameworks into the ecosystem actually improves accuracy and efficiency. Next slide

So, let's begin to talk about some of the points here of what we're looking to do as far as what we're looking for success. We actually have the verification of requestors. As I have already alluded to, the identity will be able to be provided by any number of digital identity solutions out there, whether that is through an eIDAS framework or if that potentially is through an EV cert issued by a certificate authority.

The exact credentials of what that minimum level set would be to meet that baseline identity is something that this group could

perhaps opine upon or rely upon other governments on what they feel is sufficient.

In addition to the code of conduct, same as PWC [inaudible], where we're a little different is we have actually proposed incorporating a post-dispute, ex post-dispute resolution process.

What we are looking to do is have an ADR component where data subjects can actually file a complaint if they feel that their data has been improperly used. We've modeled this after the privacy shield. So, one of the things that we're looking to do is to take that same ADR component and provide data subjects that ability to seek recourse. I think that's something that is unique. We haven't seen that in any of the other proposals.

One thing that may be interesting, looking over to you, Mark, or some other potential bulk users sitting around the table, under the privacy shield system right now, you need to designate an ADR provider to handle complaints from data subjects. You need to designate that.

One of the things that we're looking to do is to see whether this ADR component can perhaps be integrated into that or handled by that existing data provider. So, the [idea] here is we're looking to leverage existing accountability mechanisms that some bulk users may already have.

Regarding the light touch. One of the things – much like Bart, we're probably not going to get to the demo – but as part of the operational code, we've come up with a due process rules engine that is very similar to the Crocker matrix that you discussed. So, when Steve was showing you his complex matrix, we've reduced a lot of that to operational code and we can show you how that works.

But this is what is important from a light touch standpoint, particularly for the contracting parties. Unlike the current TSG model or the centralized approach of PWC, we actually want that rules engine siting out at the contracting parties. We believe that is where that rule engine should sit. We believe that any consensus policies that are adopted by ICANN should be flagged, but then we allow the individual contracting parties to set additional safeguards or mechanisms.

Another thing that is important that we have heard from talking with registrars over the last couple of months is the need to make sure that there is an automated process. So, part of the rules engines allows for either automated or manual reviews. We empower that end contracting party who is ultimately responsible for safeguarding that data to do it.

Regarding logging and centralization. What we do is the technology we use is messaging mats where we actually log … We

have the potential to log both locally as well as centrally. So, we believe that it is important for ICANN compliance to be able to have access to a centralized log to monitor all queries that are being done, but that same log, the registry or registrar that is managing that RDAP server, will have access to that same data. So, we think it's important that the contracting party has access to the same data that ICANN compliance would have access to, unlike some of the concerns that we've had with the current DAAR discussion. Next slide, please.

So, one of the things that I just wanted to walk through here is just the couple of points showing how we're going to try to address the safeguard standards and just touch on some of the distinctions between different use cases.

Again, like PWC, we are going to have logs, federated credentials. But where we're going to do this is this is going to be done at the contracting party's gateway. So, instead of necessarily having an ICANN gateway as a central focal point or rules body, we're actually distributing or federating out that credential.

Similar to what we've heard, requests will be for one or multiple domain names. There will be no bulk but the ability to do one-off queries through the RDAP is what we've proposed.

Looking at the request for non-public data. What we're proposing to comply with, those countries that have strict data localization

laws, as also to comply with the needs of cybersecurity researchers, is we are proposing that the data by pseudonymized. By pseudonymizing the data at the registrar or registry end, that allows for the ability to be compliant with a variety of rule sets. And by pseudonymizing the data, we allow cybersecurity researchers and national cert teams to do the metadata analysis for them to identify particular security threats.

We also have the ability not only for IP owners to get the information that they want but we also recognize the vibrant, if you will, domainer community. So, we actually provide a domain name registrant if they are trying to offer a domain name for sale, to basically have a special use credential to share that with a third-party to show that they are in fact the owner of that domain name, to facilitate a safe secondary domain name sale market. Next slide.

So, what I wanted to do here is, if you get a chance to look through the software at a later date, since we're running short on time, I just wanted to do you a screenshot of how we would process a domain name.

So, one of the things that we did as part of the systems, if you go, we've actually registered a portfolio of illegal content dot-com, dot-biz, dot-info, a number of domain names where we actually had information, RDAP information, registered. We generally

tried to register with those registries that have active RDAP servers to query. But in this scenario here, this is a query of information by a cybersecurity researcher or a cert team. You'll see that all of the PII is redacted, and what instead has been replaced is a pseudonymous identifier for purposes of the registrant. This will allow for some of the analysis that they need to do. Next slide.

This is an example of what an IP attorney would get, whereby identifying their legitimate interest regarding an infringement claim. They would potentially get a larger subset of data, unlike the cybersecurity researcher. Next slide.

To point number four here, one of the things that we tried to do is we basically are looking to have this information basically delivered to an end point in a secure manner. One of the reasons that we have opted to go towards this particular delivery mechanism is we recognize that some domain name requests may not be processed automatically, that some registrars may have an out-of-band review process. So, through this, we are able to basically queue up the request and have that be looked at in a secure, legally compliant manner.

As I noted before, every request is pseudonymously logged by the contracting party and could potentially be [unmasked] if a data subject wishes to bring an action. Next slide.

So, again, just on the point of fostering innovation and competition. Everything about our system is about fostering innovation and competition. The ability for PWC to come in and be a verifier in this framework is an option. The ability for DNIC through their [ID for Me] system to come in and be an identity provider, assuming they meet certain minimal criteria. And this is something I was discussing with Andreas in Amsterdam. MojeID with CZ.NIC, they actually have done a similar thing.

So, what we're looking to do is to take that identity and allow certain credentials to be attached to it. What we see that as an opportunity is for other value-added services. So, when Donuts with the Motion Pictures Association came up with their own RPM, that is a credential that could be added to the base identity for purposes of doing it.

There's been talk about trusted notifier programs in other frameworks. If in fact you are a trusted notifier, that credential can be attached to your digital identity. So, what we're trying to do here is take a much more holistic approach of doing something.

I think one of the criticisms of the Trademark Clearinghouse was you had a single-use credential that had one purpose and not much other. What we want to do here is figure out how these identities can be so much more, and again just kind of looking out

where there's the potential for future opportunities, the ability for a national trademark office to potentially digitally sign a trademark and then have that be the basis to replace the Trademark Clearinghouse and save money and increase efficiencies. These are some of the things that I think are important.

One of the final things I'll note here is, during my discussions, I've made reference to contracting parties, contracting parties. I did that intentionally, not to mention registries or registrars, because I believe the framework that we're talking about here potentially could be a basis for solving the privacy-proxy implementation because the ability for that contracting party to disclose that data in the same framework I think is, again, something that's important. Next slide.

Final takeaways. Again, focused on data privacy. Obviously, we are trying to look at the entire ecosystem of users, not just IP attorneys but potentially cybersecurity researchers. Again, we're looking to foster competition and innovation. We're not looking for proprietary solutions.

One final point that I would like to make is one of the things that's very important about the [ID for Me] initiative by DNIC which a number of community members are a participant, including GoDaddy, [ID for Me] actually proposes to use the DNS as a trust

anchor. I think this is something that's very interesting. As a community, I think we should be looking at how we can reinforce the importance and significance of the DNS in what we do, and as identity is a growing importance in other areas, I think this is an excellent opportunity to bring that about.

So, I will stop and take any questions. Come on, there has to be one question.

UNIDENTIFIED MALE: Michael, just to let you know and everybody else, we still have about a little less than about 27 minutes left, so you will have time to do a quick demonstration if we [inaudible]. PWC as well.

MIACHAEL PALAGE: Okay. Frank, do you want to come on up? Go ahead.

GEORGIOS TSELENTIS: You presented a certain moment that the requestor provides an attestation for the legal right to process the data. Can you elaborate a little bit more on that? Who tests how this attestation is produced?

MICHAEL PALAGE: So, as far as the attestation, while we originally went down the route of a federated open ID [inaudible] system, one of the things

that we've incorporated in is a PKI element. So, in order to follow-up on the attestation, looking at global e-contracting and e-commerce laws. So, when there is an attestation, you're basically digitally signing with a PKI digital identity. That's one of the things that we think is consistent with the eIDAS framework. Does that answer your question?

GEORGIOS TSELENTIS: I was more asking about the attestation about legal rights, so who is the one who attests there? I'm asking not about the process. I'm asking about the legal entity that provides this attestation is compliant all over, worldwide. If I understood this.

MICHAEL PALAGE: So, the simple answer is, depending upon the requestor, there is a list much like in Crocker's matrix or in our thing, is it pre-litigation? Do you have a subpoena? Do you have litigation? So, depending upon who the requestor is, there would be a set of legitimate interests on what they would be able to request. And they would identify that. That not only would be logged, but in fact, passed to the contracting party for them to review before processing.

UNIDENTIFIED MALE: So, put it this way. You want to split … Whatever time is left, we'll split equally? What do we have left? We have 25? So, do you want to take 10 minutes? Frank, come on up.

FRANK CONA: Good afternoon, everybody. I'm Frank Cona, InfoNetworks. I'll share my screen here. Just make some room here. Everyone can still see, okay, great.

As Mike mentioned, we have an operating system that right now just illustrates several of the policy and other decisions that still need to be made by this group and others.

What you're looking at right here is a mock-up of one of the unified disclosure gateways that we created. This could be any gateway at a contracted party, as Mike mentioned. You can authenticate into this gateway using your credentials.

For purposes of this, we've used [WebAuthen]. You can use any type of credentialing system or authentication system that you need. What I'm doing now here is I'm typing in. I don't know if people can see me on the screen. I'm just typing in my username and password here. Oh, it's my username, there is no password. I'm authenticating these in my biometrics.

Okay. So, now I'm into the system. This is an example of a request form that could be based on templates, [inaudible] to the policy

decisions that are made. So, in this example, as Mike mentioned, we have several domain names that we have registered that I'm going to submit requests for. Then we're going to select the type of IP that's in this example that it's related to. This is an IP requestor that I've logged as, so I have an IP-based form. The forms can actually be customized based on the type of credential and the type of requestor. I specified in this case trademark information. Of course, this can be any type of information that's required to prove lawful basis and legal right.

So, in this case, I'm going to select a designated lawful basis and I'm going to designate the level of legal right. This could be, in this example, it's either general research, [inaudible] investigation, discovery and existing litigation, subpoena or in a criminal event, a warrant just as examples. So, I'm picking [inaudible]. Obviously, I'm making attestation as to what I'm providing here, everything is true and accurate. This can be done in a number of ways. It can be digitally signed, for example, using PKI. Submitting this request.

Now, the request has been submitted to the appropriate contracting parties for processing based on the domain request. Now, this portal that I'm showing right here is our mock-up of any identity provider, as Mike mentioned during his discussion, this is an open system and the idea is to foster identity services across

the community but this is just used for illustration processes. This is a mockup of an identity provider that we created.

Now I'm going to log in here in the same manner that I did to [inaudible] using the same federated credential. Now, in this example, the report that I submitted before had been fully processed – or have been processed, I should say – and are now available in my inbox. We're showing delivery at the IDP for the requestor. Of course, it can be delivered to anywhere as allowed by policy.

And the format of these requests, obviously these could be provided in a number of different ways. We're just showing them in this manner for purposes of illustration.

So, if you expand this data, what you see here is all of the public RDAP data that we've pulled, as well as the non-public data that has been allowed by policy and by process.

In this example, this is automated process where the rules engine that Mike alluded to looked at the credentials of the requestor and their privilege set, looked at the nature of the request and what was submitted, and then also looked at the particular data elements and flags that could be set with respect to the data itself to make a determination as to whether to provide this data and what data to provide.

So, in this example, all of the – and for legalcontent.com – all of the data was provided because everything was cleared. In the example of the dot-net, some of the data was flagged for a manual review because the secure identifier may not be necessary to be provided – the pseudonymous identifier, excuse me – may not be necessary to be provided here. And then the rest of this data is being redacted. This could be for a variety of reasons. In this example, the nature of the registrant is such that any request for revealing their identity and location needs to get flagged for manual review.

In the third example – and this just illustrates some of the ways this can be delineated. In this example, all of the data has been redacted. In the prior example, only some of it has. The basis that is here, you can see there's a different code that's placed here. This was because there's a rule on data transfer across jurisdictions to the particular jurisdiction of this requestor.

So, just as an example, data can also be flagged to prevent onward transfer to particular jurisdictions if there's a data localization law that may impact that.

The other aspect of the system … What I can also show you is Mike mentioned the different example, where if I want to log in as a security requestor – and I've already submitted the search for

this, so we can save time with that. But I can just illustrate to you that, in this example … I'll log in as security again.

So, in this example, all of the data has been redacted except for the pseudonymous identifier, and in this case, the country of the registrant. And of course this could be designated by policy but the concept here, as Mike alluded to, is that for certain analytical purposes and other research, it may not be necessary to provide personal data but you can provide a pseudonymous identifier that can still be used for correlation and other analytical purposes to meet those needs as well, so it adheres to data minimization principles while still being able to, obviously, accommodate a variety of applications.

The last aspect of this that I'll try to share real quick is the logging. As Mike mentioned, the logs can be either centralized or retained by policy with the contracted party. So, what I'm going to do now is I'm logging into the same portal, but I'm logging into as a user that has access to the log information.

So, in this example, obviously these are centralized logs at this gateway. These could be, again, with a contracted party, they could be with ICANN. The information in these logs can be designated by policy. In our example, they are pseudonymized, so that if a data subject is part of the exposed dispute resolution process or someone for compliance purposes from ICANN or

elsewhere needed to unmask this data or get more information, they would simply click on a log. And in this example, we're just showing it could also be a request process to get this data similar to the registration data.

Then, if I go back to the [My IDP] example that we're using, that information will have been delivered to that authorized party who was able to see that data. I apologize for my fat fingers on the typing here. So, here's an unmasked report and the personal data is here.

One last point to make on this is that this data is not actually [resident] at the authorized party. This is actually still residing with the [My IDT] but it's processed in real-time to provide the access to that information as needed for purpose of this.

I do have more to show but I'm sensitive to the time, so I want to make sure you guys have enough time here.

BART LIEBEN: Okay. Because quite a few of those features are similar on our platform, what I'll focus on here is how to design the templates that we talked about where we have basically made an overview of the different datasets that can be provided in the context of a GDPR or other privacy law compliant requests.

So, what you're seeing here is a view of, for instance, a registrar that could work then on a centralized system or [MVP] 1 or MVP [2] where it's decentralized where they can perfectly operate the technology on their own systems, servers, what have you.

At this point, for purposes of the demo, we have a trademark owner, we have a security expert, you have law enforcement agency. So, for that capacity, they can set different rules and they can do that for different TLDs. So, as a registrar, you can set different requirements or different aspects, elements, to be disclosed. For gTLDs, if there's a uniform policy, but also for the different ccTLDs if they come across.

So, with respect to trademark owners, so here we're going to have the assumption that the authentication has been done. Here, for instance, for dot-com, we're going to select one of those use cases and we say, for instance, for a law enforcement agency for enforcement and fraud, we're going to look at what PWC initially has determined as being the baseline template. So, what type of information are you going to provide? You will see that admin, tech, and billing is still here for the moment. Well, I would say to keep it as broad as possible.

Let's say, for instance, in this scenario, we have determined as an organization that it is perfectly possible to provide that type of information. The registrar can then say, okay, we're going to

overrule that baseline template. I'm going to do something else with that information. So, I'm going to say that, in that case, only the domain name and the registrar name is going to be provided. Then we can also see for that scenario which template is currently active.

So, this system basically allows you to swiftly respond to potential issues, as I mentioned. If a DPA of country X would say in this particular scenario you can only provide a much more limited number of information, at that point in time can centrally push this not only if it's a centrally managed system, but also we can push it out to registrars and registries who have their own instance of this platform.

So, that's how you determine on a per-use case basis. Yourself, as a registry/registrar, whether you're going to allow the baseline or whether you're going to do a different step which you think is more appropriate or more compliant or more fitting to your own specific posture as an organization.

If you then, as a requestor, would log in, you would basically say, "We're going to look for a domain name." You key that in. So, we have one particular one. Say, for enforcement fraud. That's the case that we selected. You can provide a [inaudible] justification in which case you get manual processing.

So, we've included this step because we've envisaged a possibility. I'm not saying that is going to be the policy but it is the possibility that the requestor would need to pay for resolving the request. Of course, before they get anything, they want to know whether there's something there. So, here the requestor will see whether the registrar and/or the registry are allowing that particular piece of information.

For law enforcement agencies, bearing in mind that there could be secrecy of investigation, they don't want to disclose for which reasons they want to have access to non-public domain name registration information, they can for instance say if the report that is being logged, that log will not be available for registry and/or registrar or anybody else for a specific timeframe, in days or in months. So, that's an option that we've made available, having discussed this in quite detail with a few of the law enforcement agencies.

And then you log the request and basically you get a real-time answer that comes back – this is dummy data, of course – from registry and registrar, where we say this is the information that is done on display. This information is being logged, as I mentioned, so there's a track and trace of where it comes from. There's an IP address that is being logged from the requestor, just to make sure that it is a legitimate request coming from the person acting in the capacity that he or she is claiming to be, as authenticated by

an authentication body which could be PWC which could be anyone who meets the specific requirements.

In that sense, as we mentioned, it is currently set up as a centralized system which makes it a bit easier to do all the testing, but it's a module platform so it depends. Registries may choose to have their own instance of that system or they may choose to rely on the centralized body, in which case we can provide end-to-end assurance on the entire process and the fulfilling of those requests.

Are there any questions in this respect? We're still well within the time. Good.

RAFIK DAMMAK: Yeah. We are doing well with the time. Thanks for those demos. I hope that was useful for the team to see an implementation and also I understand your thinking to create those systems.

So, let's see if there is any question or comment. I think what we will do is just have a break before our next session. We should reconvene … Sorry, you wanted to ask? Okay, in the Zoom, but okay. Go ahead.

HADIA ELMINIAWI: Thank you so much for both presentations. I don't know if it's appropriate to ask this question or not but if you could – both of you or any of you – point out the main differences between the two approaches of the system, of the two proposed systems. Because there is of course a significant difference in approach.

UNIDENTIFIED MALE: There are a number of differences, but I think if you want to distill it down – and Mike alluded to this when he was talking – is that our approach leverages the existing framework and system we have in the community. It's decentralized. It leverages existing technologies, existing platforms in the way the systems work today and the way the parties – contracted parties and others – all work together today. So, there is no centralized [need]. They're certainly centralized, compliance oversight, that sort of thing – governance. But in terms of the system operation, it layers on top of the existing systems. If I had to point to one key difference, I think that's it.

BART LIEBEN: I don't think that it's any different. As I mentioned, we currently have a centralized system which is our [MVP] 1 and we can perfectly decentralize that, incorporating existing technologies which we've been looking into, of course, in order to do that authentication step.

I think the main difference is that our focus is very much on how do you fulfill – how do you receive and fulfill – a compliance request? So, our starting point, which is basically key if you look at GDPR and if you look at all the new laws that are popping up, that you say you have privacy by design. So, we'd be looking at how can we protect the privacy of the registrant? This is our key premise.

Then, we've been looking at technology on how that could be implemented. So, we've not started from technology. Our start was how do we log and fulfill a compliance request.

As I mentioned, we've made that approach from a global perspective. So, GDPR is, of course, important because that was the trigger to most of the impressive amount of work that you've been doing here, but you have to look elsewhere as well. I think the key there is that we can provide end-to-end assurance on the entire process. So, not just on the authentication part, but also on how do you fulfill those requests and make sure that the process remains compliant.

So, as I mentioned in the example I gave, if country A comes up with a new law, well then you need to make sure that the system is also compliant with that new legal system. This is something where you then can say, "Okay, let's launch a new EPDP version,"

however or whatever in order to see to which extent that law can be incorporated.

What we can do is we can sit on top of that to get that oversight and make sure that, as of day one, contracted parties are compliant. I think this is the main – if I would indicate one key differentiator between the proposal of Mike and WIPO and his team, it's that. We can provide the assurance. That's what we're doing and that's what is our bread and butter, basically.

FRANK CONA: There is another distinction. And just to make sure I understood you because I'm not sure – certainly, obviously, I demoed the technology here, but our system is based on policy and law and obviously is adaptable. So I'm not sure if I see that as a distinction, because certainly, that's at the root of all this for everybody.

But one of the things that brought to mind for me is the [exposed] dispute resolution component that Mike had alluded to, which as he mentioned, was built on the privacy framework, privacy shield framework. We actually incorporate that legal process and concept into the system itself, so it's holistic. It's not just focused on the technology but there is a process built in for the data subjects to lodge a complaint, and I mentioned with the unmasking process, that's built on a similar request process. So all of this built with the same kind of legal underpinnings with the

idea of obviously not being just compliant with GDPR and other data privacy and data protection regulations but also accommodating other interests, the legitimate interests for this data as well. So it's more holistic. But certainly the regulatory compliance is at the heart of it.

BRIAN BECKHAM: Just to build on what Frank said, one of the things that was an important consideration for us was to the extent we can validate the existence of IP rights and issue a token that would be a piece of the disclosure puzzle. We didn't think it was appropriate for us to then also be assessing where there was a claim that that data was misused. So, the idea was that any compliance takes place outside of the accreditation framework. There's a dispute resolution process and whatever the result was. If the agent was deemed to have exceeded the scope of the authorization for the data they received, then we would just get a message to revoke their tokens so they wouldn't be able to participate with that token anymore.

RAFIK DAMMAK: Okay. Thanks. We have a time check here. We already reached the end of this session but I think we have Margie in the queue, so giving her the chance to ask a question, hopefully a quick

response, and then I think everyone is looking forward to the break.

MARGIE MILAM: Thank you very much. Both very interesting presentations. I have a question about how you accredit the IP holders I guess from the PWC side, and also any thoughts from either of you on how you accredit cybersecurity professionals.

BART LIEBEN: Well, I think with respect to the IP owners, quite a few people in the room have been involved into the dot-EU process where we did accreditation verification about 346,000 IP-related claims. So, we have quite a mature process in place for that, so that is definitely possible to do it. It's I think still the most successful sunrise period that has ever took place. So, I think with respect to IP owners, we can go beyond as we did in dot-EU – beyond registered trademarks. It's also the unregistered trademarks that are important. It's all types of intellectual property rights that we faced with, and also on a very international scale.

With respect to cybersecurity professionals, well, what we've been looking into is, for instance, the licenses that are being given, the certifications that have been given, which could certify a certain cybersecurity specialist as being past a certain exam,

obtained a certain title, certain degree. So these are elements that we would take into account. There could be re-certifications afterwards. Quite a few of those certificates that are being issues by cybersecurity bodies are renewable, so that's for instance something which we would follow-up. I think at this point we have something like 60 or 70 of those accreditations listed in our system, against which we can start doing verification. As being one of those components.

FRANK CONA: And from our perspective, to answer that question, the verification process we believe – and Mike alluded to this – should be done by the organizations that are best situated to do that. So, in the case of intellectual property, obviously WIPO is involved with that process. For cybersecurity, the other associations, organizations that would be better positioned to do that.

Our approach – and this was a point we made earlier – is that it opens the system up to all of those as authorizing parties. So, for certain types of credentials, like cybersecurity, there are cybersecurity related associations that can be part of this and use the system for that process. Part of the demo we didn't get to is that we actually illustrate in there. In the case of WIPO, if you want to make a request, you already have your identity right from there. You can submit a request to be qualified. In addition to the

base information, there would be information about your organization, whether you're working individually or with an organization, what that is. Certain credentials, if you're an attorney for example, what jurisdictions you practice in and that sort of thing, so that could be verified. Similar to processes that are used today for getting credentials on the IP side, there would be a similar … And by the way, as IP owners – and Brian had talked about this – also you could submit your set of IP and say, "This is my basis for the credential based on my ownership of this IP," because that may also, as you build out the request process, that may factor in as well for certain types of requests. So, we support that also.

Then, on the cyber side, there would be a set of verifying criteria that are going to be built into the code of conduct that are obviously going to come up via policy to do that, but it would be by the organizations that are best situated to handle that.

RAFIK DAMMAK: Okay, thanks. Thanks, again, for the demo and the presentation. We'll close for this session and we'll reconvene in ten minutes which will be our last session for the day before Thursday. So, please be on time. I know that it's too cold here and everyone needs to warm up.

Okay, everyone, we should reconvene in one minute, so I will ask everyone to take their seats. We just have I think just one hour for the last session in trying to continue our deliberation and prepare for Thursday, so please take your seat and let's start quickly.

Thanks. So, this is our last session for EPDP today. I hope that you all got warmed up outside. What we are trying to do is to continue our deliberation on the safeguard entry, but what we should avoid here is to focus on the language or wordsmithing. It's more about thinking of any missing input or anything we should add here. So, I would ask everyone to think about this.

What we also do is will continue getting this input and the staff will work in an updated version to be shared later for review and to prepare for Thursday meeting. So, let's focus really about anything we think is missing here. If there is any discussion, specific discussion, on what has happened before we are taking notes and we can work later on as to even a small group of those interested to find a solution.

I remember that since we cut the queue in the morning session and we had at the time Ashely and Margie, so I want to give you the opportunity to make your comments. Let's go with Margie and then come back to Ashley.

MARGIE MILAM: Actually, I forgot what I was going to say, so I think it's fine. I actually just wanted to see if anyone wanted to have some follow-up dialogue on what we just saw just to see if we had any impressions or observations while we've got those presentations fresh on our mind.

[MARK SVANCAREK]: To be more specific, since we've been talking about safeguards, did these presentations – did it make us feel better about the safeguards we have in place or did it show a need to add more safeguards? I'm trying to bring this back in line with what we were actually doing during the day before we were having presentations.

RAFIK DAMMAK: Thanks, Mark. I hope you are not asking me this question.

[MARK SVANCAREK]: Sorry. Yeah.

RAFIK DAMMAK: Okay. Just joking here. So, we have Thomas and Stephanie. I saw you. You don't need to wave like that. Okay. One of you should start. Stephanie?

STEPHANIE PERRIN: Thanks. Before we talk about safeguards, let's talk about the risk assessment. I don't think we really saw a risk assessment in either of those presentations and they're introducing a pile of new risk.

If there's one thing that I registered from SSAC's remarks, forcefully made by Patrick at the standards workshop that we did in Barcelona, is that you don't move the data. So, both of them were suggesting moving the data, so … Among many other risks.

RAFIK DAMMAK: Okay. Thanks, Stephanie. Thomas?

THOMAS RICKERT: I simply wanted to make the point that I was unclear what the purpose of the presentations was. I hope that you don't perceive this as criticism. Let me try to explain. If this is just for information purpose, that's one thing. But we are trying to craft a policy which can be the basis for an implementation and it looks like we've had presentations that are implementations of an access model, of whatever shape or form.

If, at the end of the day, we come up with the policy, then it will not be for our group to do the procurement process for a third-party vendor that can help with the technical implementation.

So, I was unclear whether ICANN has potentially identified these providers with potentially helping with a solution so that we have to take into account some of the design features that they have offered and presented into our thinking [inaudible] policy, and if this were true, then I think we should try to write it up and make sure that we actually deliver on that task. And if this is not the overall goal, then I think we should try to tease out – and maybe we can do that here maybe later from the notes – what design principles we need to build into our own processes. I think that this is part of what Mark has alluded to. We had a little chat outside during the break. I think that some of the ideas are great to inform our thinking in terms of processes, with tokens and all that. But I would just like some guidance from hopefully you or staff on which way to go with this.

RAFIK DAMMAK: Okay. Thanks, Thomas. I think it's like what happened before with the presentation from Steve Crocker is you had groups, they made a request to the chair about they want to present what they did [inaudible] new system or the approach they followed. And I think here it's kind of input for us that we might or not use it. Depending if we see it can be helpful for us.

I can understand the concerns but I think if we give here the opportunity to hear from other parties, they want to share the

work they are doing or the solution they are thinking, as we did probably before when we engaged with the TSG and so on. But I think I can clarify this has nothing to do with ICANN Org. It's just the request comes directly to the working group – I mean, the EPDP team leadership.

But at the end it's really up to us as a team to see if it's useful, if there is anything that can help us. Probably what the idea, maybe it's kind of visibility, prototype, or [MVP] that was said many times. But at the end, for us, we have a clear task [and one to do]. I guess, Marika, you wanted to add more here?

MARIKA KONINGS: Thanks, Rafik. Just to add I think it was really that latter thinking of indeed what are some of the design principles that the group may need to factor in. And at least what I took away as well, I think it clearly shows that what is really the implementation of what we're looking at, and I think it crystalizes even further what are the policy questions that the group needs to address. So, I think it may also help as part of the conversation to really make sure that the group focuses on the policy recommendations and the policy principles and leave the implementation for that path but at least I think it gives an idea of what a model may or could look like. And we've already seen different variations of that. So, I think the real hope from our side, and I think as well from leadership,

was that this would inspire the group's thinking about how to approach the questions. What are really the key issues that need to be addressed and what are some of the elements that are actually really more implementation and can be done in different ways? Of course, the group can always provide implementation guidance but it's really a matter of doing that in the second phase, basically, or the implementation phase.

RAFIK DAMMAK: Okay. Thanks, Marika. Thomas, does that respond to your question? Okay. Sorry, I'm checking the queue here. I know that you were in the queue in the morning and you wanted to make a comment, so I'm checking here if you still want to intervene. Sorry, Margie, you wanted to make a comment? I was asking Ashley, too.

MARGIE MILAM: Oh, I'm sorry. I didn't want to jump the queue there if others were ahead of me.

RAFIK DAMMAK: Okay. So we can come back to you later. We have James, Kristina, and Milton. James?

JAMES BLADEL: Just very briefly. Can we expect anymore of these presentations, these model presentations? Do we have anymore scheduled for Thursday or going forward? I think this was the concern that I raised about opening the door a little bit, that this would be a never-ending process and we can see how much time we've already spent on this. I'm not saying it was wasted time. I'm saying it's precious time.

RAFIK DAMMAK: Thanks, James. As far as I know, I don't think we received other requests of this type. I guess in this discussion, we can reconsider about this, if we need to have it in the future. Kristina, then Milton.

KRISTINA ROSETTE: I'm going to go a little further than Thomas and James and put a little finer point on it. I think it would be appropriate to the extent that other third parties want to make presentations to us that they provide us with pre-recorded presentations that can be made available to us through the Wiki so we can watch them at our leisure instead of using either meeting time or this extraordinarily valuable face-to-face time. Thank you.

RAFIK DAMMAK: Okay, thanks, Kristina. Milton?

MILTON MUELLER: Yes. I'm yielding the floor again to Stephanie.

STEPHANIE PERRIN: Kristina has already made my point. I was going to make it a little more pointedly, but she was more eloquent.

RAFIK DAMMAK: Okay. Thanks, Stephanie. Margie?

MARGIE MILAM: I think I look at it from a different perspective. I think it helps us understand what's possible and helps inform our policy discussions. I'll give a couple of examples. We're talking about safeguards. Someone talked about an ADR component to this that helps the data subjects. I think that's something we can explore from a policy standpoint. Having some sort of verified credential that relates to the different types of requestors like IP or cybersecurity, I think that's a pretty good idea. So I think it actually can help us inform what we come up with. It doesn't mean we have to go with either of them and what their approach was but I don't think it was a waste of time. I just think it's something that we can explore.

The other thing I thought is relevant from prior discussions is the notion that perhaps these systems could be self-funded, if you will, that it's not going to be incumbent on the contracted parties to create the software to implement something like this. We heard that from both of them, that they were willing to come up with a business model that would essentially be funded I guess through perhaps accreditation or whatever but we haven't learned the details yet.

Anyway, those are takeaways from what I saw and I don't think it was a total waste of time, but I agree that we probably don't want to spend much more time on it.

RAFIK DAMMAK: Okay. Thanks, Margie. We have Ashely and then Mark.

ASHLEY HEINEMAN: I won't belabor it because I agree with what Margie just said. I think all that being said, this has been really helpful presentations. I don't think we need anymore at this point. And I think in the future definitely avoid face-to-face sessions because I think the beauty of it is for us to have a conversation face-to-face and we kind of detracted from that.

Also, I just wanted to flag – and I apologize for being late this morning – just to note that in the GAC input to the EPDP, this is

actually something that we call out, what we see anyway as kind of a chicken and an egg syndrome that we have going on in the group where [you] want to know what additional policies there should be and we're trying to work towards policies, yet we're very reluctant to talk about what the actual model will be. It's kind of hard to propose policies to consider when we don't really know what we're working around.

So, if we can find ourselves in a position where obviously we're not going to be picking any of these models but they all have very similar approaches and I think it's going to be helpful in guiding our work moving forward.

RAFIK DAMMAK: Thanks, Ashley. Mark?

MARK SVANCAREK: I think I'm not entirely repeating what everybody said. I do think there was some value to these presentations because it does help us to establish what the state of the art is. Theses things have been prototyped in only a few months, so it's interesting to see that. That said, I really don't think we need anymore of these. I think we're well-informed now of what the state of the art is and I do like Kristina's idea that if we do have to have more that having

a pre-recorded self-serve format might be more valuable. Thank you.

RAFIK DAMMAK: Okay, thanks. I guess we can close discussion on this matter. As far as I know, we don't have any additional requests of this type, so I don't expect that will come up again anytime soon. I think we are taking note of all those comments and see what's the best approach. I'm not going to say to avoid wasting time, like how to be more effective and to have this in a way that's really useful for the team. Yes, Stephanie. Please go ahead.

STEPHANIE PERRIN: Thanks, Rafik. I just wanted to point out that, in my view at least, some of the implicit assumptions about who's going to pay for this are flawed. The actual volume of access requests, if you leave out access to billing data, is very low. There is existing guidance from the data commissioners on what you can charge for such access requests that will constrain any great designs on paying for this system on the backs of the registrants in it, and therefore I think we should gather our stats on how many access requests we're getting, just so that we don't walk down this path again. Thanks.

RAFIK DAMMAK: Okay. Thanks, Stephanie. Just to be sure, Brian, you want to add something on this topic? Substance, that's good. So, I said let's continue the work for input on the safeguards. So, Brian, please go ahead.

BRIAN KING: Sure. Thanks, Rafik. Let's make sure that we're getting credit for the homework that we've done in the safeguards section, so when a third party – I hate to use third party. When somebody else looks at this later. I suggest that we put a placeholder for now that says that the GDPR safeguards are in place, like data minimization principles and those things that we've already gone through in the first phase of the EPDP have been noted and are a part of the safeguards around this data processing. So, I'd like to put a placeholder for now and we can spell those out I think later is my suggestion.

RAFIK DAMMAK: Thanks, Brian. I don't see anyone else in the queue. So, just to be sure here, we know that we discussed several items under the safeguard entry and I think there are some discussions, some part of them but maybe changing the language for deletion. So, as I shared before is the idea is for you to have many a new version later on based on all this input so we can prepare for a Thursday meeting to continue the discussions. So, I'm here asking if you

think there is anything missing and you want to add. This is a good chance, so we can add in the new version and we can, to some extent, move the discussion. Yes, Alex?

ALEX DEACON: To answer your question, I can't think of anything at the moment to add, but can I make a comment about suggested update to existing bullet points that we haven't discussed yet?

RAFIK DAMMAK: I mean, it's something we didn't discuss yet as a bullet point.

ALEX DEACON: Yes. I mean, it was mentioned briefly earlier but I've been thinking about it.

RAFIK DAMMAK: I think it's possible if it's [inaudible].

ALEX DEACON: So, I was thinking about the conversation we had earlier about these three bullet points – the no Boolean, the no search, the no reverse lookups – and the statement from Alan G that we should avoid implementation questions, future-proofing, if you will our policy. So, I'm wondering if it makes sense to replace those three

bullet points with something along the lines of lookup and/or search functionality shall be limited to the capabilities of RDAP. Basically, pointing out the technical limitations of RDAP but not ruling out future additions that we're not currently contemplating but we may see later on. So, just a thought on that.

RAFIK DAMMAK: Thanks, Alex. So, we have James.

JAMES BLADEL: So, just off the cuff, Alex, I think that we would probably be opposed to that specific language because RDAP, to my understanding, does have those capabilities – some of those capabilities. So it would have the impact of essentially just taking those bullet points and reversing them and adding the positive in, that if we limit it to the capabilities of RDAP and RDAP has these pseudo-surveillance features, then that wouldn't be something that we could agree to. Thanks.

ALEX DEACON: Yeah. I appreciate that. Is there a way we could reference RDAP profiles that are approved via the various consensus policies or EPDPs? For example, implementation of RDAP is constrained currently by the work that's being done in the RDAP profile working group – and again, I don't know off the top of my head

how that's implemented and/or enforced, but would additional language along those lines help, James? Constraining it to decisions made here at ICANN versus just RDAP in general.

JAMES BLADEL: I have to talk to … We're editing on the fly again, which I hate. But I think the key here is that the WHOIS system never had those functions or features. Those were offered by third-party data aggregators. So, to build those into an ICANN RDS system – data access system or even a policy – I think we should start from the position of where we left off with the WHOIS system when it essentially went dark and not start to build in the features and functions that were offered by third-party data services.

But let us talk about it. I get your point, which is we're trying to not close the door, I guess. But we are trying to close the door because we're trying to draw a demarcation because what WHOIS used to be and what other this sort of cottage industry of repackaging and reanalyzing WHOIS data used to offer and not pulling that in under the RDS RDAP SSAD umbrella. But I think we need to confer on that. I think my personal position is that these are important functions, both in a policy and technical function, that allowing requestors to pivot searches on data fields and essentially then follow those data fields throughout the DNS I think raises a number of concerns.

ALEX DEACON: Maybe we could take this offline and I could think about it more and put some language onto the list. I'm definitely not suggesting that we take it that far. I'm just trying to future-proof this a little bit and maybe even those words are inappropriate and could be worded better. I'm just trying to think about this a little bit. I'll think about it and propose language that maybe we could discuss on the list and we'll all have time to go back and chat with our constituencies.

RAFIK DAMMAK: Thanks. So, I guess this is an action item and to follow-up later on. So, I guess that's an old hand. I see Milton and then Alan Greenberg. Milton?

MILTON MUELLER: Yes. We're still on the same bullet point, although I am noticing here that accredited parties are not provided with bulk access has been crossed out. We never agreed to that. We, in fact, debated it at some length and I would like to see that un-crossed out. It's okay to add a note that some of our group do not want that there. That's fine. But we did not agree to have crossed that out.

That relates to the other three bullet points that Alex was discussing. I think James already hit this point, which is that we

know what had happened with the old WHOIS. Basically, the data was vacuumed up, value-added services were sold to people which gave all of these functionalities, based on the assumption that this data was not protected in any way, and we want to make sure in terms of specifying safeguards that that doesn't happen again.

So, we want to be very clear about these kinds of things that are not going to be part of the system and we're a little bit nervous about the fact that those points are being gone after by Alex and others because that reinforces our concerns that people are trying to recreate the old WHOIS with this new RDS.

So, I'd be happy to look at any wording changes that Alex is willing to propose on the list. If there's a better way of saying this, that's fine. But bear in mind why those bullet points are in there.

RAFIK DAMMAK: Okay. Thanks, Milton. Alan?

ALAN GREENBERG: Thank you. Maybe I'm living in a different world but I think we should be keeping this as simple as possible, and if the current WHOIS only allows searches based on fully formed domain names, then just say that. We don't need all the negatives of what isn't involved if we make it really clear in some simple sentence

what isn't allowed. And if all we're allowing is full domain names, no wild cards, then why do we have to add all the other parts?

RAFIK DAMMAK: Okay. Thanks, Alan. Margie?

MARGIE MILAM: I forgot. I'll go back in the queue when I remember.

RAFIK DAMMAK: Okay. Margie, I'm worried about all these memory problems. Let's go to Mark and then Brian.

MARK SVANCAREK: Yeah. Right now the bullet is just weird to some of us. Bulk access isn't defined in a way that makes it distinct from the other bullets but since we have these real concerns that are being expressed, let's just note that we are going to replace this with better language and that Alex and I are at least on the hook for that. I'm willing to help with that as well. I do think that this should be pretty easy to come up with. A smaller set of bullets that expresses the points of all parties.

Like I had mentioned, here's a scenario that could be defined as bulk access, even though it's asking for one domain at a time. I'm

just doing it rapidly. So, we'll just clean it up. So, for now, just put the asterisk next to it that Alex and I will clean it up and then …

RAFIK DAMMAK: Okay. So, I think [inaudible] action item [inaudible] to work or clean it up, change the language. Can we set some deadline? Because it would be really good to have all this before our meeting on Thursday. So, Alex, I don't know if you can coordinate and get this done as soon as possible. Yes, Marika?

MARIKA KONINGS: Thanks, Rafik. I think staff is also happy to take it as an action item here to try to address all the comments and suggestions that have been made with an updated version that we could probably circulate by the end of today, and then those that have agreed to work online which I had specific concerns, can then take whatever we did and either redo that, change it or maybe they like what we actually put forward based on the discussion. Maybe that's the way, where there is an updated version but people can react to that and provide their specific suggestions.

RAFIK DAMMAK: Thanks, Marika. I think it was mutually exclusive. So, we'll have an updated version but also some item that we have some volunteers to work on to get that as soon as possible in the way

that people are aware about the change, and if we can include them to the updated version.

Okay. We are back to Margie. I hope now you remembered what you want to say.

MARGIE MILAM: Sorry. I do remember. Logging – is that a safeguard we want to put in? That came up in the presentation today. I think we do auditing/logging requests as a safeguard. Okay.

The other point, I wanted to reply to Milton. This was basically a strawman. It didn't represent any sort of consensus in the group. So, as you say, we don't agree. Well, I think on the flip side, there's probably a lot of us that agree. We could say the opposite, that there was no consensus to put it in in the first place, so I just think we need to be really careful when we're looking at the template that this wasn't reflecting a consensus discussion among us, whether anything should be in there is open to debate and not just taking things out. So, that's something I think we need to keep in mind. Thank you.

RAFIK DAMMAK: Okay. Thanks, Margie. Just to double check, Brain, I thought you were in the queue. Okay. Let's see if there is any further comments. So, we have I think 35 minutes left and we are trying

to make use of this in the way that we can prepare for Thursday to be effective and efficient on that day.

So, what we are expecting is to get an updated version hopefully by today. Yes, Marika?

MARIKA KONINGS: I just want to note, of course, that only focuses on the safeguards section and some of the other suggestions made. I don't know if we have time to look at some of the other ones or at least get an indication of some of the other areas, which ones are maybe the most problematic ones or what are issues. Again, if there are ones that need further conversation, if we don't get to that today, if people can submit their either suggestions or concerns to the mailing list it would really help us as well shape the agenda for Thursday's meeting.

RAFIK DAMMAK: Yes, Marika. We think for now that's all what we get for safeguards. We can try to move to one of the entries. But also that reminded me regarding sharing comments and input in the mailing list. We started now with this use case and I hope everyone thought [inaudible] other use cases, so it would be really good to share them also as soon as possible, so to see if we have time to discuss them or to give opportunity to the team

members to review them [inaudible]. So, just highlighting this. If you already discussed or you are thinking about some use cases that we can add to our list.

Okay. If no further comment or anything to add for now for safeguards, let's see what maybe we can start checking as an entry. Sorry, can you scroll up? Let's see which, maybe something that we can start with. If we can get a quick [inaudible]. Let's check. Any suggestions? Thomas says maybe I was not clear.

So, I think for now, for safeguards, we got as much as possible for input and we will have a new version. Maybe there are also some [language] to work on, but I think for now I don't see any further comment, so the thought is to use the time – we have like 30 minutes left – to go one of these entries on the template. I was asking if anything you can think we can start and it's not controversial or something we can discuss within the 30 minutes. That doesn't mean that we need to finalize now. Any suggestions? Yes?

THOMAS RICKERT: Why don't we double check whether the headline, the use case … I think Alex had an amendment to the language which I consider friendly because it also copies the language in the GDPR – trademark owners processing data, the establishment exercise or

defense of legal claims for trademark infringement. Maybe we can just double check whether that is controversial. If not …

RAFIK DAMMAK: I guess we can do that. Let's check.

THOMAS RICKERT: Because if not, then we can move on.

RAFIK DAMMAK: Okay. Thomas, do you want to comment on something else or?

THOMAS RICKERT: I think, I would hope that, A and B are more or less un-controversial. I think there have not been any comments on that before. We should probably talk a little bit about lawful basis and then the set of data that's being disclosed. That could be …

RAFIK DAMMAK: All this within 30 minutes, Thomas?

THOMAS RICKERT: Yeah.

RAFIK DAMMAK: Okay. In the meantime, I think Marc is in the queue but we can do that.

MARC ANDERSON: Thanks, Rafik. I was going to suggest maybe in the time remaining take a look at F, accreditation of user groups. That one – I know that might be a bigger topic than the time we have left and I don't know if people are prepared to really dive into that one but that one might be one of the more interesting topics to spend some of our face-to-face time on.

RAFIK DAMMAK: Okay. We have two suggestions here, either to … Okay. But anyway I think we'll start the deliberation but it doesn't mean we have to finish today. So, if we can start, that's okay.

So, we have it shared on the screen. Let's see if anyone wants to comment or intervene here. I can give you one or two minutes just to read it quickly. I see, Alex, you want to comment.

ALEX DEACON: Yes. On the first point – and I haven't had a chance, I was just doing that when you called on me. At a minimum, I think we should make sure we at least cover all of the items that we put in rec 18, the reasonable access rec in phase one. I was going to do

a compare and contrast but it seems – there's only two things here. I thought we had more. I think that would make sense to me, at least, as a starting point. At least start with what we've already decided, if it makes sense, which I think it does.

RAFIK DAMMAK: Thanks, Alex. I see Margie and then Amr. Margie?

MARGIE MILAM: Yes. Regarding the issue of attorney's agents, I think we also need to add service providers because the brand protection companies like Mark Monitor that do a lot of this work for us and that's standard in the industry, so we want to make sure that we also pick up the service providers.

UNIDENTIFIED MALE: Is that not the same as an agent?

MARGIE MILAM: I don't know if it's necessarily an agent or not, but I just want to clarify it, so there's no confusion that they're able to … As long as there's a letter of authorization that they're able to submit requests on our behalf. Thank you.

RAFIK DAMMAK: Thanks, Margie. Amr?

AMR ELSADR: Thanks. Just revisiting the point I made earlier today, and I guess now is a more appropriate time to make it. It would be helpful I think to understand what the benefits of accreditation are and what some of the risks might be, especially some of the scenarios I described earlier, whether an agent or attorney, whether authorization is withdrawn or whether a marks owner loses the right to use that mark. And whether these might be outweighed by some other process other than accreditation, which is not terribly burdensome on third parties seeking data disclosure. It's not what I'm trying to achieve here. I'd just appreciate at some point – we don't have to do this now – but we have a discussion about this and explore different possibilities. Thanks.

RAFIK DAMMAK: Thanks, Amr. Kristina?

KRISTINA ROSETTE: It could be that my eyes are still frozen, but Alex, on the point that you made about rec 18 and adding that in, what was the other category that you were talking about?

ALEX DEACON: I don't know. Again, I haven't had a … Maybe my intervention was premature, but I hadn't had a chance to back and look at what we had agreed with in phase one to make sure it was, at a minimum, covered here. I didn't have anything specific in mind. I could do that. I think the comment to the side that Marika put I think is a good starting point and we could follow-up.

RAFIK DAMMAK: Okay. Thanks, Alex. Just double checking here, Amr, is it an old or new hand? Okay. Georgios?

GEORGIOS TSELENTIS: Yes. Looking at the template there as we have it, I think what is below furthermore refers to codes of conduct for this accreditation. So, whereas the first two parts refer to the evidence of the accreditation. What we have underneath furthermore, agree to only use the data, only issue disclosure, etc., all this part for me looks like we are referring to codes of conduct, whereas the first part is more about assuring about the accreditation of the user groups and we provide this assurance by the evidence and the letter of authorization. I don't know if this distinction is helpful for our analysis but I want to point out that.

RAFIK DAMMAK: Okay, thanks, Georgios. I just want to check something. Marika, you want to say something? I see the green check. Okay. Brian and then Alan.

BRIAN KING: Thank you. I think the data processing agreement that we're talking about here is a really good idea. I want us to be careful when we use the words code of conduct, Code of Conduct with capital Cs is defined under GDPR is, to my knowledge, not something that has ever been done yet. So I don't want to set us up for failure and march down that road if it's not something that we'll accomplish in a reasonable timeframe, if at all, because like I said, I don't think it's ever been done but certainly agreement to process the data in compliance with GDPR and these safeguards is a good idea. Thanks.

RAFIK DAMMAK: Okay. Thanks, Brian. So, we have Alan Greenberg and then Alan Woods.

ALAN GREENBERG: Thank you. I'm going back to the previous section on evidence of ownership. The UDRP applies to non-registered trademarks and a host of other trademarks that you can't provide us a single sheet of paper of evidence, so I'm not quite sure how that will be

covered here. But just evidence implying there's a piece of paper saying you own the trademark is probably not something you can produce in many cases.

RAFIK DAMMAK: Thanks, Alan. Alan Woods?

ALAN WOODS: Thank you. I may break the mold and I agree completely. I almost took my hand down. I agree with Brian on the code of conduct point. It's very important. Then I slightly disagree with him. I think that we should be aiming – and this far too far in the weeds for now but this is something we should be focusing towards as a code of conduct, and just because it hasn't been done in the past doesn't mean we can't [inaudible] that trend. So, let's focus on that in the future, I think.

RAFIK DAMMAK: Okay. Thanks. Thomas?

THOMAS RICKERT: Yeah. In response to Alan Greenberg, the limitation to registrant trademarks was intentional because if you want to have an easy to carry out process that can potentially be automated, for registered trademarks, it can just ping against the database of the

patent and trademark office and establish that the mark exists for common law trademarks and stuff like that. It's not that easy. So, maybe you have ideas on how that can be implemented but this was intentionally limited to what is in the document.

And on the use of the terminology of the code of conduct, I do agree with both what Brian and Alan have said, but the term code of conduct – and this is what Georgios I guess referred to, but it's subject to his confirmation – is that ICANN in its previous documents has raised the idea of a code of conduct to be abided by those who want to get access to registration data.

So, I think ICANN has put us into this predicament that we are using a term that is a legal term under GDPR for something that was not meant to be a code of conduct according to Article 40.

So, I think what we need to work on – and in that regard, you are spot on – we need to have principles or rules or what have you that would give you the eligibility to be part of this process, and maybe we should use that term instead of code of conduct because I think that – and I think I've said it on other occasions on this team – ultimately we should try to get our policy recommendations transformed into a draft code of conduct that will hopefully get the blessing of the authorities because that will give ultimate legal certainty and avoid the risk of being

sanctioned if you play by those rules for the contracted parties, plus ICANN.

RAFIK DAMMAK: Okay. Thanks, Thomas. Yes, Stephanie, please go ahead.

STEPHANIE PERRIN: Just to clarify, when I talk about procedures, that's what I'm talking about. We might want to entertain the thought of having binding corporate rules which is different than a code of conduct, right? Not to get into a nerdy discussion.

THOMAS RICKERT: Let's take that offline, with the BC [inaudible]. I think it's a good idea but we need to think it through whether it's the best thing for this scenario.

RAFIK DAMMAK: Okay. Thanks. So, just double check, Alan Woods, is it a new or old hand? Old, okay. So, James?

JAMES BLADEL: Thank you. Just to make things more confusing, I understand that code of conduct is a term here and it is a term of art in GDPR and other privacy legislation. It's also mentioned in reference a

couple of times in our Registrar Accreditation Agreement. So, I think that it's very important for us that if that language survives into a consensus policy that it be clarified that it is not the code of conduct that is referenced in the RAA and does not, therefore, get back-doored into an ICANN compliance obligation on contracted parties. Really, just registrars I think. I don't think you guys have that in your agreement.

I know we're talking about different things, but we're calling them by the same name, so we need to be careful that we're making that distinction. Thanks.

RAFIK DAMMAK: Okay. Thanks, James. So, we have Margie, Brian, and Hadia.

MARGIE MILAM: I think we need bullets on what – I don't want to call it code of conduct. Basically, an agreement, an accreditation agreement, what you have to agree to abide by, how you're going to treat the data. There's a lot of things we're going to have to flush out but it's what would be in a code of conduct but it's just not called a code of conduct. It's a contract. That's what I envision when we're talking about this.

RAFIK DAMMAK: Okay. Thanks, Margie. Brian?

BRIAN KING: I don't want to confuse us any further, but if we do – I won't then.

RAFIK DAMMAK: Okay. I guess it's the confusion topic. So, we have Hadia.

HADIA ELMINIAWI: I was wondering how this first sentence "agree to only use the data for the legitimate and lawful purpose" described above different than the sentence that we added in the section of safeguards, if we can go back to that. Yeah. Where is it? Proof/statement of use or non-use of data objectives. How is this different from the one put further down? Don't they both in the end lead to the same thing?

KRISTINA ROSETTE: Can I jump in? Because I think this might have been a follow-up to the point I raised this morning, maybe.

RAFIK DAMMAK: Yes. Please, go ahead.

KRISTINA ROSETTE: Although I apologize because I think I may have had to step out during this. The short answer, Hadia, is no, that the first in terms of the accreditation is a condition of the accreditation, whereas this is really more in terms of the safeguard intended to go to whether or not the requestor, after having requested and received disclosure of the data either used it or didn't use it. So, it's intended to go to different objectives.

HADIA ELMINIAWI: But you have the user in the very beginning agreeing already to do that, right? So, he already agreed. So, he does it twice? He agrees before and after?

KRISTINA ROSETTE: The requestor would have to agree that they would only use it for the purpose for which it was disclosed, right? Then, later, they would, after having received the data, the intention here, the objective – I don't want to say purpose – would be to have them confirm that they either did use the data or they didn't. And if they did, the presumption is that they used it only in connection with the lawful purpose.

HADIA ELMINIAWI: You could assure this through any kind of auditing that you're doing, simply. You have the requestor from the very beginning

saying, "I'm going to use the data for this purpose." That means he's going to use it for this purpose. After that, you can make any kind of auditing to assure that it happened.

KRISTINA ROSETTE: Understood. But the auditing is after the fact and puts the obligation on either the contracted party or the operator of the system and the intention here is to put the obligation on the requestor, the party requesting and receiving disclosure of data.

RAFIK DAMMAK: Okay. Thanks, Kristina. Brian?

BRIAN KING: Thanks. I see a really high level of risk – unacceptably high level of risk – on the requestor here, from a legal perspective. If we're put in a position to say what we did or didn't know and then what we did or didn't do with the information that we had, that's a real tricky legal position. I think it's really inappropriate to require the requestor of the data is investigating potentially a legal claim to show to someone – we don't know who and we don't know for what purpose and with what safeguards – what we knew about or might have known about infringement or what was happening on a website. That's a really tough place legally and I don't think it's appropriate here.

RAFIK DAMMAK: Okay. Thanks, Brian. Quick one?

ALAN WOODS: How is that any different to the risk you're asking us as contracted parties to take on? In fact, maybe we could just share that [inaudible].

BRIAN KING: I can respond. I think it's a different risk altogether. I think we're talking about data protection and data privacy risk that we're trying to establish here and help to minimize and trying to show that the requestor of the data, whether for trademark or other purposes, knew something and then had to prove that they did or didn't do something about what they knew. Those are legal decisions that an attorney and a client sit down and make and that are very in-depth decisions that a company makes and a company or any other kind of requestor. It's a very different kind of risk than privacy law risk.

ALAN WOODS: My response to that would be surely that's a legal assessment that you would do before you request the data. The receipt of the data is not going to change your mind as to whether or not you're

going to take that particular risk. It's a bigger conversation, but no.

RAFIK DAMMAK: Okay. Thanks. I mean, it's good to highlight any concern or issue for now but of course that needs to be continued. So, time check. We have roughly ten minutes left. I think we still have more to discuss and we will continue Thursday. But just wrapping up and maybe to see if there is any other business. Just double checking to see if we have any action items and reminders about the next steps to Thursday. Marika? So, I said [inaudible], so if there are any action items. Maybe that's usually Caitlin. Maybe reminding about the next steps towards Thursday, so people should really prepare for that session.

MARIKA KONINGS: Thanks, Rafik. I'll hand it to Caitlin, but the ones I remember by heart, I think we have an action item to update this template based on the comments received today, and in a number of cases, make suggestions which of course all of you then have an opportunity to review. Everyone is as well encouraged to provide any further input on any of the sections that were not discussed and preferably in the form of either specific suggestions for changes or specific concerns, so again we can use them to help build the agenda for Thursday's meeting.

I think there were also some groups that were working on other use cases. I think the GAC was working on a public safety one. I don't know if there's any chance that that could get delivered to the group before Thursday, so if we have time, at least we would be able to run through it and start thinking about it. I think groups should also start thinking about further use cases that need to be developed. I think we're probably sort of settling on the template and approach. Again, I think it's really important to, by Thursday's meeting as well, have an idea or at least a list of use cases that need to be developed and owners for those, so that we can work towards those in a future meeting – meetings.

And I think one last point. For Thursday's meeting, there's also an engagement planned with ICANN org and specifically the project team that will be liaising with this group as well as with DPAs on some of the questions in relation to the UAM based on the TSG model. So, they're coming in for a conversation. So, if there are already any specific questions you have for them or any points you would like to address, feel free to share those as well ahead of time, so we can pass them on and make sure we can have a constructive discussion. I think that's everything I have on my list.

CAITLIN TUBERGEN: Thanks, Marika. I just wanted to note one other additional action item. That is that any group who has not yet provided their early input, please do so prior to Monday, July 8th. Thank you.

RAFIK DAMMAK: Thanks, Marika and Caitlin. So, I guess we can have here any other business. It seems, Thomas, you want to start here.

THOMAS RICKERT: Thanks very much, Rafik. I think that I would have one proposal. I think it's good that other groups are starting to think about the population of the template for other types of queries. From what I read in the chat and from what some of the interventions, I got the feeling that our group is still not aligned on what the process should look like.

Let me at least share my thinking. The idea would be that we have standardized queries to which all the criteria that we discussed will be attached. And if all the requirements that are established are fulfilled, then there can be an automated processing of those queries. That's at least the goal that I had in mind. Because there was the ongoing debate about the balancing test and whether you can anticipate balancing tests and stuff like that.

So, let me be very clear. My hope is that we can have, for these standard scenarios, that we can have prefabricated balancing

tests that we would conduct and say, "Okay, if the query looks exactly like this, if all the parameters are present, then the data can be disclosed." For this one, as I mentioned when I introduced or presented this template, it was relatively easy. We will have other disclosure scenarios where the balancing test will not be as easy and straightforward.

So, I think it would be extremely good if we had a group of volunteers probably working with [Brad and Bert], if resources permit, to work on a standardized methodology for conducting the balancing test which would be just one field, in this one, but actually we would need to go through different questions when conducting the balancing test where it has to be present. And I think it would be good to have one single standardized approach for doing that, with some legal counseling – not necessarily legal advice but just help from outside counsel for us to get a methodology together that will likely past muster if ever tested.

So, that's my suggestion for Thursday. I will not be there on Thursday. Unfortunately, I have to leave in the morning. But if you would like me to help with anything in terms of engagement with the authorities, I'm more than happy. So you can volunteer me on Thursday if you wish to.

RAFIK DAMMAK: Thanks, Thomas. Be careful for what you wish. But point taken, and I think we can see if we can follow this approach as you suggested. James?

JAMES BLADEL: Thanks, Rafik. James with another AOB item and this is something completely out of left field. And I want to mention that I have not cleared this with my colleagues from the contracted party [inaudible], so buckle up.

Many of you may be aware or probably maybe not aware that there is a group that is actively lobbying and advocating in Washington for a legislative approach to many of the same problems that we're addressing in this PDP, namely the collection and dissemination and access to registration data. If this group were to succeed in what are their stated goals, it would effectively undermine our work here and essentially make this effort irrelevant.

So, I think it would be worthwhile for this group to, for the record, establish that we believe that approach is working against our interests here in ICANN and here this group that we've established and put together and that we would essentially disavow the national level legislative approach to the WHOIS or the RDS challenges that we're discussing. And I think, furthermore, just to reinforce the good faith of everyone here, I

think it would be good for any individuals or groups in this PDP to distance themselves or disassociate themselves from any of those efforts because it starts to look like folks are taking parallel paths to the same – I don't know that that's happening. I'm just saying for the avoidance of doubt.

So, I'd like to put that on the table. This is something I've been saving for our face-to-face. Unfortunately, I won't be here on Thursday, so I have to drop this bomb as we're all leaving the door on Tuesday. But it's something that I'd like this group to consider, as there are at least one, and perhaps other groups, that are out there kind of working against us. I think that we should, and perhaps jealously, protect our charter and protect our mandate and protect our reason for existence. Thanks.

RAFIK DAMMAK: Okay. Thanks, James. Point taken here. I think, Thomas, that's an old hand. Thomas, is it an old hand? Okay So, I see we cleared out the queue and we have two or three minutes left. Thanks, everyone, for participating in today's sessions and we will continue on Tuesday. But in the between, we are expecting your input and comments on the mailing list and also some volunteers work together on some language to be shared with the team. Okay, thanks again, and the meeting is adjourned.

[END OF TRANSCRIPTION]